

# HAKING

PRACTICAL PROTECTION

DIGEST

## HACKING ORACLE

PROTECT YOURSELF FROM  
ARCHITECTURAL FLAWS

50+  
PAGES

SECURITY IN AN  
ORACLE DATABASE

SECURE YOUR COMPANY'S  
NETWORK WITH THE  
JUNIPER NETSCREEN NS SERIES

IDENTITY THEFT

ORACLE'S ACHILLES' HEEL  
- ATTACK, DEFENSE AND  
FORENSIC RESPONSE

Vol.7 No.10  
Issue 10/2012(58) ISSN: 1733-7186

PLUS

READING BETWEEN THE LINES  
- THE ARTICLE BY MALWAREBYTES'  
ADAM KUJAWA





# Protected Only by Antivirus?

Complete your PC's security by running Malwarebytes  
Anti-Malware alongside your Anti-Virus to become fully  
protected from the latest threats.

## Protect Your Business Now!

Visit [Malwarebytes.org](https://Malwarebytes.org)



For more information,  
Contact us at [Corporate-Sales@Malwarebytes.org](mailto:Corporate-Sales@Malwarebytes.org)





# Atola Insight

That's all you need for data recovery.

Atola Technology offers *Atola Insight* – the only data recovery device that covers the entire data recovery process: *in-depth HDD diagnostics, firmware recovery, HDD duplication, and file recovery*. It is like a whole data recovery Lab in one Tool.

This product is the best choice for seasoned professionals as well as start-up data recovery companies.

## Emphasized features at a glance:

- Automatic in-depth diagnostic of all hard drive components
- Automatic firmware recovery and ATA password removal
- Very fast imaging of damaged drives
- Imaging by heads
- Case management
- Real time current monitor
- Firmware area backup system
- Serial port and power control
- Write protection switch



Visit [atola.com](http://atola.com) for details



## HAKIN9 team

**Editor in Chief:** Ewa Dudzic  
ewa.dudzic@hakin9.org

**Managing Editor:** Ewelina Soltysiak  
ewelina.soltysiak@hakin9.org

**Editorial Advisory Board:** Rebecca Wynn,  
Matt Jonkman, Donald Iverson, Michael Munt,  
Gary S. Milefsky, Julian Evans, Aby Rao

**Proofreaders:** Michael Munt, Rebecca Wynn,  
Elliott Bujan, Bob Folden, Steve Hodge,  
Jonathan Edwards, Steven Atcheson, Robert Wood,  
Ewelina Soltysiak

**Top Betatesters:** Hammad Arshed, Amit Chugh,  
Viswa Prakash, M.Younas Imran

Special Thanks to the Beta testers and Proofreaders  
who helped us with this issue. Without their assistance  
there would not be a Hakin9 magazine.

**Senior Consultant/Publisher:** Pawel Marciniak

**CEO:** Ewa Dudzic  
ewa.dudzic@software.com.pl


**Production Director:** Andrzej Kuca  
andrzej.kuca@hakin9.org

**DTP:** Ireneusz Pogroszewski  
**Art Director:** Ireneusz Pogroszewski  
ireneusz.pogroszewski@software.com.pl

**Publisher:** Software Press Sp. z o.o. SK  
02-682 Warszawa, ul. Bokserska 1  
Phone: 1 917 338 3631  
www.hakin9.org/en

Whilst every effort has been made to ensure the high  
quality of the magazine, the editors make no warranty,  
express or implied, concerning the results of content  
usage.

All trade marks presented in the magazine were used  
only for informative purposes.

All rights to trade marks presented in the magazine  
are reserved by the companies which own them.  
To create graphs and diagrams we used [smartdraw.com](http://smartdraw.com)  
program by  SmartDraw

Mathematical formulas created by Design Science  
MathType™

## DISCLAIMER!

The techniques described in our  
articles may only be used in private,  
local networks. The editors hold no  
responsibility for misuse of the presented  
techniques or consequent data loss.

## Dear Hakin9 followers,

*This month's issue deals with oracle security and id theft. Julian Evans has prepared his column, ID Fraud Expert Says focusing on how to protect yourself from ID Fraud in the UK. We also have a special article written by Malwarebytes' Malware Researcher, Adam Kujawa, who will discuss the tips and tricks on how to get what you want from assembly code. His article, Reading Between the Lines will discuss:*

- *How to make sure you are looking at real code and not garbage*
- *How to rename subroutines so they are easy to spot*
- *How to leave breadcrumbs in the code by making comments*
- *How to work backwards by 'finding the cheese first'*
- *How to make your map complete by forcing the code to work for you*

*The article Security in an Oracle Database written by Andreas Chatzinantonou will discuss the various ways to secure an Oracle Database and prevent SQL injections.*

*Paul Wright will discuss Oracle's Achilles' Heel – in which he will outline the main weaknesses of the Oracle Database and will show how to secure against its most serious architectural flaw.*

*Douglas Berdeaux will discuss the link between identity theft and web applications, while Delyan Boychev and Ran Levi give you the details about ID theft – the risks and consequences and how to prevent this from happening. Massimiliano Sembiante from R.I.F.E.C will discuss side channel attacks with brain leading to data and ID Theft. We also have a feature on network security appliances by Chris Weber, who will discuss how to secure your company's network with the Juniper Netscreen NS Series.*

*I hope that you will enjoy reading this issue as much as the authors enjoyed writing their articles.*

*Go ahead and Get Hakin9!*

*Ewelina & the Hakin9 Team.*

## ORACLE DATABASE SECURITY

### **Oracle's Achilles' Heel – Attack, Defense and Forensic Response in A Distributed Database Estate** **06**

*By Paul Wright*

This article will highlight one of the main security weaknesses in Oracle Databases, it will then demonstrate a solution to this weakness and finally show how native auditing can be used to forensically identify the presence of this attack in a large distributed estate using a centralised syslog audit trail.

### **Security in an Oracle Database** **10**

*By Andreas Chatzinantoniou*

This article shows how the various security features of the Oracle database work and how you should deal with your data in a secure way. Chatzinantoniou discusses how to secure data at rest and how to prevent SQL injections.

## IDENTITY THEFT

### **R.I.F.E.C.: Digital Security and Risk Analysis – Side Channel Attack with Brain Leading to Data and ID Theft** **16**

*By Massimiliano Smbiante*

Recent development of computer science integrated with neural engineering, allow detecting and decoding of brain activities via sophisticated interfaces devices. This may expose users to serious threats. This article will provide a review of the latest researches, will summarize the techniques used to interface brain with computer and will analyze potential risk exposures.

### **Identity Information Theft and Web Applications** **22**

*By Douglas Berdeaux*

This article will discuss the importance of securing web applications and identity information. It will show how the smallest vulnerability in a web application can lead to the largest identity information breach. The author will also give security tips for database administration of CMS users and will show several web attack methods of hackers who target your data.

### **The Hidden Facts About Online ID Theft** **26**

*By Delyan Boychev*

The author will describe how you can lose your Online ID, and what are the possible risks and consequences of that

happening. The author also proposes ways of protecting yourself from such risk.

### **Identity Theft: Stay Alert, Be Suspicious** **30**

*By Ran Levi*

This article written by Ran Levi will discuss all issues regarding ID theft. The author will present to you the vulnerabilities and threats connected to ID theft and will also show you how to prevent and deal with situations where your identity is at risk.

## NETWORK SECURITY APPLIANCES

### **How to Secure your Company's Network with the Juniper Netscreen NS Series Security Appliance – Part 1** **36**

*By Chris Weber*

This month the focus is on a comparable unit from another top tier vendor that is also a great purchase in the enterprise resale market and still provides solid, fast efficient enterprise class stateful inspection at the perimeter with some advanced application layer features. The Juniper Netscreen.

## EXTRA!

### **Reading Between the Lines – How to Quickly Obtain what you are Looking for when Reverse Engineering Assembly Code** **46**

*By Adam Kujawa*

The article will discuss the tips and tricks on how to get what you want from assembly code. Kujawa's article shows you how to make sure you are looking at real code and not garbage, how to leave breadcrumbs in the code by making comments and lastly how to make your map complete by forcing the code to work for you

## ID FRAUD EXPERT SAYS

### **How to Protect Your Identity in the UK from Fraud** **54**

*By Julian Evans*

Information is being collected about us every second of every day without us ever realizing what happens to it. Most of us don't really care what happens to our personal data as long as it isn't misused. Julian Evans gets up close and personal by taking a brief glance at how you can protect your personal data if you are a UK citizen.

# Oracle's Achilles' Heel

## Attack, Defense and Forensic Response in A Distributed Database Estate

This article will highlight one of the main security weaknesses in Oracle Databases, it will then demonstrate a solution to this weakness and finally show how native auditing can be used to forensically identify the presence of this attack in a large distributed estate using a centralised syslog audit trail.

### What you will learn...

- The reader will learn how to secure against the most serious architectural flaw in the Oracle RDBMS.

### What you should know...

- Readers will have Oracle DBA/Dev, Unix and security knowledge.

If a remote user tries to guess the SYS password repeatedly using an automated tool then they are not slowed down, but for other accounts they are. This means that brute force protection is only in place for low privileged accounts not for the highest privilege account. This concept was published in an article by the Author back in 2007 ([http://www.rampant-books.com/art\\_wright\\_oracle\\_passwords\\_orabrute.htm](http://www.rampant-books.com/art_wright_oracle_passwords_orabrute.htm)).

See basic PoC in Listing 1.

So Oracle DB protects the lower privileged accounts more than the highest privileged SYSDBA account. This is one of the greatest weaknesses in the Oracle DB. For SYS it is even more important to delay remote pw guessing, because it is immune to the security that profiles bring (e.g. password complexity verification function and lockout).

#### Listing 1. Basic PoC

```
[oracle@orlin dbs]$ while true;do sqlplus -S -L sys/wrongpw@orlin:1521/orcl_plug as
                        sysdba;sleep 0;done;

ERROR:
ORA-01017: invalid username/password; logon denied
.... 8< .....snip
no failed logon delay for SYS account!

[oracle@orlin dbs]$ while true;do sqlplus -S -L system/wrongpw@orlin:1521/orcl_plug;sleep
                        0;done;

ERROR:
ORA-01017: invalid username/password; logon denied
.... 8< .....snip
failed logon delay starts for non-SYS account
```

## Defense – put a time delay on repeated SYSDBA attempts

One way to defend against this attack is to introduce a time delay to repeated guesses on the same account to slow the attacker's guesses down. Here is simplified PoC code that achieves this by adding a one second delay to every attempt. For full pro-

duction code please contact the author on paulmwright@oraclesecurity.com (Listing 2).

## Forensic incident response via centralised auditing

It is not well known is that Oracle is the only DB vendor that has the built-in ability to centralise it's

### Listing 2. Simplified PoC code

```
Create user systhrottle identified by lowsec12;

Grant execute on dbms_lock to systhrottle;

create or replace trigger systhrottle.tra_servererror_oral017
after servererror on database

declare

    l_db_usr varchar2 (32);

begin

    if (ora_is_servererror(1017)) then

        l_db_usr := upper (trim (sys_context ('userenv', 'authenticated_identity')));

        if l_db_usr = 'SYS' then

            dbms_lock.sleep (1);

        else

            NULL;

        end if;

    end if;

end tra_servererror_oral017;

/
```

### Listing 3. Oracle Syslog Audit Trail

```
Sep 28 11:37:24 oracle Oracle Audit[23714]: SESSIONID: "24523"
ENTRYID: "57" STATEMENT: "8" USERID: "SCOTT" USERHOST: "ro-rac3"
TERMINAL: "pts/2" ACTION: "103" RETURNCODE: "0" OBJ$CREATOR: "SCOTT" OBJ$NAME:
"TEST" SES$ACTIONS: "-----S-----"
SES$TID: "154816" OS$USERID: "oracle"
```



audit trail *free of charge* by pushing syslog from all the Databases to a single collector. What this means is that compliance can be achieved for a large Oracle DB estate without having to spend money on a third party logging solution. This article will now show you how to do this based on the experiences of a large scale rollout. This is what the oracle syslog audit trail looks like: Listing 3.

The forensic signature for a remote brute force attack on SYS is as follows. The 1017 status code is specific to the failed logon and there are multiple attempts at the same time for the SYS account, which shows someone is trying to brute force SYS access into the DB (Listing 4).

It may be the case that the syslog audit trail has been compressed into gunzip format on Unix as this results in great disk savings. The compressed audit trail records can then be searched using commands like the following.

```
for file in */*/*.gz; do gunzip -c "$file"; done |
    egrep -i '1017'
```

READ MORE about running OS syslog commands and configuring the Database syslog in our full issue.

#### PAUL M. WRIGHT

*Paul M. Wright is an expert at securing 3-tier Oracle architectures, with over a decade of experience, including Pentest Ltd, NGSSoftware, Betfair, Markit Group and J.P. Morgan Investment Bank. This experience includes secure software development, deployment, configuration, monitoring, logging, forensic response, compliance audits, architecture and research leading to credit in 5 Oraclequarterly Security Alerts. He is Author of the first book on Database Forensics and has been published in IOUG's SELECT Journal, UKOUG's SCENE Journal and presented original research at ISACA, RSA, ISSD and SANS. Paul currently holds OCP for DBA and Development having already taught the first Oracle and Java Security courses for SANS in the UK. His current security work is for Oracle's 12.1 DB Beta and can be viewed through his blog at [www.oraclesecurity.com](http://www.oraclesecurity.com).*

#### Listing 4. Attempt to brute force SYS access

```
[root@localhost ~]# tail -f /var/log/boot.log
Mar  9 00:26:40 localhost Oracle Audit[15819]: LENGTH : '162' ACTION : [7] 'CONNECT'
          DATABASE USER: [3] 'sys' PRIVILEGE : [4] 'NONE' CLIENT USER: [6] 'oracle'
          CLIENT TERMINAL: [5] 'pts/1' STATUS: [4] '1017' DBID: [10] '1229390655'
Mar  9 00:26:40 localhost Oracle Audit[15823]: LENGTH : '162' ACTION : [7] 'CONNECT'
          DATABASE USER: [3] 'sys' PRIVILEGE : [4] 'NONE' CLIENT USER: [6] 'oracle'
          CLIENT TERMINAL: [5] 'pts/1' STATUS: [4] '1017' DBID: [10] '1229390655'
Mar  9 00:26:40 localhost Oracle Audit[15823]: LENGTH : '162' ACTION : [7] 'CONNECT'
          DATABASE USER: [3] 'sys' PRIVILEGE : [4] 'NONE' CLIENT USER: [6] 'oracle'
          CLIENT TERMINAL: [5] 'pts/1' STATUS: [4] '1017' DBID: [10] '1229390655'
Mar  9 00:26:40 localhost Oracle Audit[15827]: LENGTH : '162' ACTION : [7] 'CONNECT'
          DATABASE USER: [3] 'sys' PRIVILEGE : [4] 'NONE' CLIENT USER: [6] 'oracle'
          CLIENT TERMINAL: [5] 'pts/1' STATUS: [4] '1017' DBID: [10] '1229390655'
Mar  9 00:26:40 localhost Oracle Audit[15827]: LENGTH : '162' ACTION : [7] 'CONNECT'
          DATABASE USER: [3] 'sys' PRIVILEGE : [4] 'NONE' CLIENT USER: [6] 'oracle'
          CLIENT TERMINAL: [5] 'pts/1' STATUS: [4] '1017' DBID: [10] '1229390655'
Mar  9 00:26:40 localhost Oracle Audit[15839]: LENGTH : '162' ACTION : [7] 'CONNECT'
          DATABASE USER: [3] 'sys' PRIVILEGE : [4] 'NONE' CLIENT USER: [6] 'oracle'
          CLIENT TERMINAL: [5] 'pts/1' STATUS: [4] '1017' DBID: [10] '1229390655'
Mar  9 00:26:40 localhost Oracle Audit[15843]: LENGTH : '162' ACTION : [7] 'CONNECT'
          DATABASE USER: [3] 'sys' PRIVILEGE : [4] 'NONE' CLIENT USER: [6] 'oracle'
          CLIENT TERMINAL: [5] 'pts/1' STATUS: [4] '1017' DBID: [10] '1229390655'
Mar  9 00:26:40 localhost Oracle Audit[15847]: LENGTH : '162' ACTION : [7] 'CONNECT'
          DATABASE USER: [3] 'sys' PRIVILEGE : [4] 'NONE' CLIENT USER: [6] 'oracle'
          CLIENT TERMINAL: [5] 'pts/1' STATUS: [4] '1017' DBID: [10] '1229390655'
```





"knock knock ...  
Bugtraq has you ..."

## Feel the new revelation

*The distribution known as Bugtraq-I, emerged from an independent project of two young enthusiastic Spanish guys. Noted for its easy use and easy configuration. Technically it is a stable and agile system in which applications are all automated and where the user can monitor all services of the system in real time.*



Christian González and Rubén Galán creators of Bugtraq-1

### Why choose Bugtraq-I?

There are multiple reasons, but the most notable one would be the global vision of the system that the user has with the conky interface. The friendly desktop makes an easy environment for a newbie user. Bugtraq-I is adaptable to any situation of ethical hacking.



### Which applications/tools can you find in Bugtraq-I?

First of all, the majority of actual pentesting and forensic tools are incorporated in this system. These include tools of Windows that also work in Bugtraq. Next to that, you can find new branches of malware and anti-virus, with the purpose of empowering this unusual branch in GNU/Linux. Another type of tools are those that have been created by the Bugtraq-team. Lastly, Bugtraq-I also contains scripts for the installation of tools that require the user configuration, making a personal system in just a few minutes.

### In which system is it based?

Bugtraq-I is based in Ubuntu 10.04 with the kernel 2.6.38 generic-pae. The desktop

environment is based in Gnome 2, optimized for the best performance.

### What do you mean with automated applications?

One of the main differences between the actual pentesting distributions is that not a single unnecessary service runs in Bugtraq-I. Everything is thought through in such a way that the system intelligently selects the needed services to make the application work; like this the user monitors in real time all the daemons of the tools.

### How to install?

You can download Bugtraq-I Final from official website. You can install it from a dvd or usb, where you have the option to use it liveCD or use the installer directly.

### Are you planning to continue this project?

Yes, of course. We have created a private community in which we are developing new tools and giving the opportunity to grow to unknown or unsupported projects. The inscriptions have been closed on July, so if somebody want to participate, we will give 10 places for the readers of hackin9.

#### Internet Contact

**Website:** [www.bugtraq-team.com](http://www.bugtraq-team.com)

**Twitter:** @BugtraqTeam

**E-mail:** [staff@bugtraq-team.com](mailto:staff@bugtraq-team.com)

#### Pre-Inscriptions:

[inscriptionsh9@bugtraq-team.com](mailto:inscriptionsh9@bugtraq-team.com)

# Security in an Oracle Database

The most important asset of a company is their data. Losing customers addresses, orders, payroll information, research data, medical data or credit card numbers can easily become a major disaster for each organization. Naturally you want your data to be secure in various ways, be it, its access, its integrity, possibilities to backup and restore it in secure ways, encrypt it and so on.

## What you will learn...

- Various ways to secure an Oracle Database
- Secure data at rest
- Prevent SQL Injections

## What you should know...

- No prerequisites required
- Examples are self-explanatory

**T**his article shows how the various security features of the Oracle database work and how you should deal with your data in a secure way. On the other side this might also act as a (initial) checklist for the security conscious in order to see if the current security regime is up to its task.

To be honest, the Oracle database offers thousands of features of features, and most of them cover security in one way or another. Complete books have been written and they only give a glimpse, so the intention of this article is not to be complete but to give you a starting point into the journey around Oracle Database Security.

## Basics

Oracle has a more than 30-year long history with its database, and with the CIA as one of its first customers it is not a surprise that security has always been a prime concern. Nowadays, the number of main security features covers a number of thick manuals, and tightly integrates with diverse topics like (Enterprise) Identity Management, Application Security and secure backups.

To come up with the biggest point up front, it is difficult to compromise a vanilla installation of the Oracle database, and next to impossible to penetrate a well configured database. Does that mean we can move on and look for other systems that

might have more vulnerabilities? No – Oracle releases security patches frequently, although not all target the database.

## Users

Two kind of users exist in a database: administrative users such as the *Database Administrator* (DBA) have accounts (SYS, SYSTEM) and normal users (called schemas). In a basic version a user is administered inside the database, created by the SYS users and granted certain rights.

```
sys@orcl> create user andreas identified by
welcome1 default tablespace users;
sys@orcl> grant connect to andreas;
```

With these rights, the user “andreas” can get into the database and can pretty much do nothing. In order to access data, you need the right to select data from a table.

Now as data is stored in relational tables, the user cannot simply select or modify them. Before *that* can happen the SYS user needs to grant certain rights on the table itself. But rights can also be revoked.

```
sys@orcl> grant select, insert on emp to andreas;
sys@orcl> revoke delete on departments from
andreas;
```



This system of grants is applied on all objects inside the database. The default is – obviously – that you have no rights. Of course a concept of groups exists as well. The above examples are still valid, but today it is typically only used for application specific users, as since the advent of three-tier-architectures no “real users” access the database directly.

Users can be administered externally – for example in an LDAP server. Unfortunately a direct integration with AD does not work, but with some features of the Oracle Identity Management Suite this is possible.

### Administrator

So, as you cannot access the database without a normal user, you might want to use a different way to get access to the SYS account. As with all IT systems that have users with elevated rights, the SYS user is probably the most vulnerable part of the database. Evidently, the SYS user can do everything inside the database. What you want to accomplish is to lock out the SYS user from user data. Imagine a tablespace (where the data tables reside) contains confidential data that even the DBA is not allowed to see (e.g. credit card numbers). In this case you want to ensure that the DBA cannot access the data. Oracle offers an option that makes sure that the SYS user cannot access these data. This option is called “Database Vault”. In essence the database becomes a no-go area for the DBA, except for the essential system data that makes the database itself work.

With Database Vault you would secure a tablespace using a web-based application, based on realms on which the security can be defined. When the SYS user tried to access data of a table the following will happen:

```
SELECT FIRST_NAME, LAST_NAME, SALARY FROM  
HR.EMPLOYEES WHERE SALARY >10000;
```

Error at line 1:

```
ORA-01031: insufficient privileges
```

The main concern with this security feature is pretty obvious: configuring the Database Vault is typically done by the DBA. So the DBA could go in there and temporarily disable the Database Vault, do his mischief and switch it back on.

Luckily, such an action will trigger an auditable event inside the database. Auditing in itself is a basic functionality of the database, however it is normally disabled, as a full blown database in action

Learn  
Web Application Security  
with...



## Coliseum

Virtual labs  
100% practical hands on  
training  
by eLearnSecurity

**FIND OUT**

14 educational challenges

- ✓ Real world scenarios
- ✓ No set-up time
- ✓ Play on MS SQL Server
- ✓ Got stuck? We support!

will create an enormous amount of auditing information, which will have a negative impact on performance.

So the DBA is locked out from production data. Are we safe now, when using the Database Vault? Nope, as the audit information remains inside the database, which the SYS user could get rid of as well. Are we in a situation that the SYS user is really locked out? No, but there is another database option that will catch the DBA red-handed. The Database Audit Vault comes to our rescue. Audit events – even switching the auditing on or off – will be shipped in a secure way to another database. If you make sure that the second database is not managed by the first DBA (but for example by the Internal Oversight Committee / Auditos/Internal Affairs) you are done. You cannot prevent the access completely, but at least you have forensic evidence that something has happened.

## Storage

Good, so users and DBA are covered. So – a villain might just open the data file and try to read the data directly.

```
root> dd if=/u01/oradata/orcl/order.dbf \
      ibs=8192 skip=3449 count=1|strings

1+0 records in
3449+0 records out
Andreas Chatziantoniou 1234432112344321 435.32
                        1305.96 Gizmo 3
```

So apparently someone ordered three Gizmo's worth 1305.96 Euro using a credit card with the number 1234432112344321.

How can we protect the data when it is at rest (on the disk)?

The database offers two possibilities for this: data encryption and Transparent Data Encryption (TDE).

Data encryption needs to be used in the application, for example as shown in the following PL/SQL block (very abbreviated): Listing 1.

With a key you can encrypt or decrypt data before you insert it into a table. Problem as usual is the key management. Such a key needs to be available in the program, so either it is hardcoded or stored in a wallet. The wallet technology resem-

### Listing 1. Example of DBMS\_CRYPTO (abbreviated)

```
G_CHAR_SET VARCHAR2(10) := 'AL32UTF8';
G_STRING VARCHAR2(32) := '12345678901234567890123456789012';
G_KEY RAW(250) := utl_i18n.string_to_raw
                  ( data => G_STRING,
                    dst_charset => G_CHAR_SET );

G_ENC_TYPE PLS_INTEGER := dbms_crypto.encrypt_aes256
                          + dbms_crypto.chain_cbc
                          + dbms_crypto.pad_pkcs5;

FUNCTION enc_creditcardnr( i_ccnr IN VARCHAR2 ) RETURN RAW
IS
    l_ccnr RAW(32) := UTL_I18N.STRING_TO_RAW( i_ccnr, G_CHAR_SET );
    l_enc RAW(32);
BEGIN
    l_ccnr := utl_i18n.string_to_raw
              ( data => i_ccnr,
                dst_charset => G_CHAR_SET );

    l_enc := dbms_crypto.encrypt
              ( src => l_ccnr,
                typ => G_ENC_TYPE,
                key => G_KEY );

    ...
```



# Get the best real-world Android training anywhere!



Attend

## AnDevCon IV

The Android Developer Conference

December 4-7, 2012  
San Francisco Bay Area

Choose from more than 65 classes and workshops!



- Learn from the top Android experts, including speakers straight from Google!
- Attend sessions that cover app development, deployment, management, design and more
- Network and connect with hundreds of experienced developers and engineers like yourself

AnDevCon is the biggest, most info-packed, most practical Android conference in the world!

## Register Early and SAVE BIG!

[www.AnDevCon.com](http://www.AnDevCon.com)

Follow us: [twitter.com/AnDevCon](https://twitter.com/AnDevCon)

"AnDevCon is a fantastic conference! There is no better place to experience the latest and greatest technologies and techniques in the field of Android development. If you attend one conference this year, this one should be it!"

—Jay Dellinger, Senior Software Engineer, Manheim

A BZ Media Event

AnDevCon™ is a trademark of BZ Media LLC. Android™ is a trademark of Google Inc. Google's Android Robot is used under terms of the Creative Commons 3.0 Attribution License.

bles the way in which Java or Apache store keys, however there is only a graphical interface for this.

A better alternative is to use the Transparent Data Encryption. With TDE the complete datafile is stored in an encrypted way. The following snippet shows how to create such a secured tablespace:

```
CREATE TABLESPACE my_enc_tbspc DATAFILE '/home
/user/oradata/my_enc_tbspc.dbf' SIZE 10M
ENCRYPTION USING 'AES192' DEFAULT STORAGE(ENCRYPT);
```

That means that the above example of the root user executing a “dd” command will deliver just garbage. Naturally, for the TDE a separate key is needed. Often companies combine the access mechanism to the key with a smart card. So only when the DBA is on site, the smart card is inserted into the reader, otherwise the card is put into a physical vault (banks do this as they have the infrastructure and certain applications that will operate only during certain hours). Therefore stealing the disks and trying to restart the database on a different computer will fail, as you miss the wallet with the key.

Now we know that the data is safe inside the database and even when it is on the disk (at rest).

As a smart hacker you then want to try the back-up media (often enough these are still tapes, although they became less popular). Access to tapes, especially when they are stored off-site is dangerous. Now a similar technique can be (optionally) deployed with backups: secure backups – which mean that the backup data in itself is encrypted again. So only when you have access to the wallet you can restore the database. This poses an organizational issue, as you need to ensure that a copy of the wallet is stored in a very secure location on-site and off-site as well.

**READ MORE** about secure access of the database, SQL injections in our full issue.

## ANDREAS CHATZIANTONIOU

*Andreas has some 25 years of IT experience, of which the last 14 were exclusively spend with Oracle Technology (Database, Application Server, WebLogic Server, Fusion Middleware). Having worked for Oracle and Accenture and other companies, Andreas is now a freelance Oracle Consultant who – after all these years – thinks he partially understands the stuff he’s working with. Contact data: Andreas Chatziantoniou, andreas@foxglove-it.nl.*

### Listing 2. Configuration of the Advanced Security Option

```
(DESCRIPTION=
  (ADDRESS_LIST=
    (ADDRESS= (PROTOCOL = tcps) (HOST = my_orcl_server) (PORT = 1521)))
  (CONNECT_DATA=
    (SERVICE_NAME= creditcarddata.securecompany.com))
  (SECURITY=
    (SSL_SERVER_CERT_DN="cn=sec_guru,cn=OracleContext,c=nl,o=securecompany"))
```

### Listing 3. Usage of Oracle Wallet

```
java.util.Properties japro = new java.util.Properties();
...
// Define key store, and password
japro.put ("javax.net.ssl.keyStore", "/home/andreas/wallet.jks");
japro.put ("javax.net.ssl.keyStoreType", "JKS");
japro.put ("javax.net.ssl.keyStorePassword", "welcome1");

// Set the trust store, and password
japro.put ("javax.net.ssl.trustStore", "/home/andreas/certs.jks");
japro.put ("javax.net.ssl.trustStoreType", "JKS");
japro.put ("javax.net.ssl.trustStorePassword", "welcome1");
```



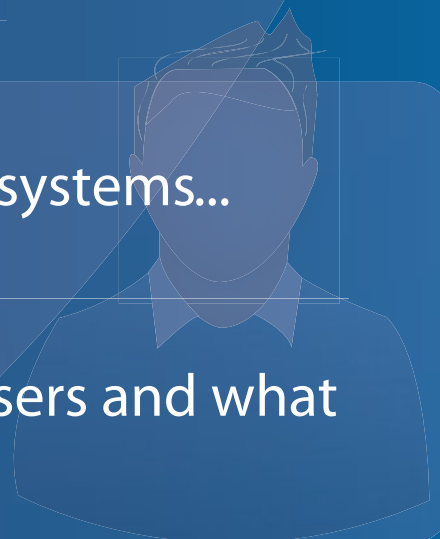
## Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...



## Be proactive...

- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...



ID Theft Protect provides information on threats from a user perspective.

Visit: <http://id-theftprotect.com>

# Digital Security and Risk Analysis

## Side channel attack with brain leading to data and ID Theft

Recent development of computer science integrated with neural engineering, allow detecting and decoding of brain activities via sophisticated interfaces devices. This may expose users to serious threats.



**T**his article will provide a review of the latest research, will summarize the techniques used to interface brains with computers and will analyze potential risk exposures.

### The beginning

Something that truly sounds like one of those futuristic, visionary Sci-Fi movies as Johnny Mnemonic is probably already a reality.

On the 8<sup>th</sup> of August 2012, a research team from some of the most renowned universities' such as: Oxford, Berkley UCLA and Geneva, announced a successful attempt to "hack" into human brains using a BCI (brain computer interface) device, with a technique similar to a Side-Channel attack.

Many people are not really aware of what this achievement may represent in terms of progress and future developments.

To have a clear understanding of what exactly is the risk we are exposed to and how the "Brain Hacking" is achieved, we need to have an overview of how the brain works and what technology has been used to attempt mind reading.

### The Brain

Our Brain is an incredible machine composed by a number of features and functions. Almost everyone is aware that Neurons (Figure 1) are fundamental cells that through electro-chemical reac-

tions allow exchanging information and performing major brain activity.

Our brain contains around 100 billion neurons. These cells are used to process electric signals.

Axons are extensions of neurons. The cell membrane of the axon contains voltage-gated ion channels that allow neuron to generate and propagate electrical signals and communicate with each other.

The ionic current flows within the neurons generate a fluctuation that can be measured and recorded using a device called *electroencephalograph* (EEG) that uses sensors applied over the scalp to detect the electric activities.

Generally the electric activity of the brain is represented by the summation of the synchronous activity of thousands or millions of neurons with similar orientation. If the cells do not have similar orientation, the ions do not line up and create waves that can be detected called Brain Waves.

Brainwaves are classified as the following:

- Beta – when the patient is alert or feels agitated or afraid.
- Alpha – during physical and mental relax.
- Theta – somnolence with reduced consciousness.
- Delta – when there is unconsciousness, sleep or even catalepsy

## The BCI – Brain computer interface

Research on BCI device began in USA at UCLA Berkley around 1970. The project was commissioned by DARPA (Defense, Advanced Research Project Agency), the same agency that supported the ARPANET project, formally known as INTERNET. After years of experimentation on animal cavy, in the mid 1990 the project announced the first successful Neuroprosthetics device implanted on humans.

Neuroprosthetic devices are neural prosthesis capable of substituting sensor and cognitive functions, generally implemented on patients affected by neural damages, with reduced or inexistent functionalities results of injuries or diseases (Figure 2).

Over the past decade, many researchers and laboratories started to explore the potentialities of BCI technology as it may be the source of a number of future applications.

Even if the BCI device seems quite complex and sophisticated, practically is based on the same concept of the *electroencephalograph* (EEG) recording brains activity from scalp electrodes, sampling signals (typically of 128 Hz – 512 Hz).

Each single variation of the electric waves is mapped and translated into performable tasks such as: controlling cursor movement, select letters or icons and so on.

The Mapping phase is important because the system requires to be previously tuned in order to interpret the signals. During the BEAM (*Brain Electrical Activity Mapping*) the BCI perform the following steps:

- Signal acquisition – user performs tasks to map EEG samples of brain activities.
- Samples Extraction – translate received signals to specific tasks

For instance, when we think or visualize an object, we produce electric activity over multiple areas, mainly because our brain is searching through our memories an association with the target object to identify it and schedule the next activity.

The process of sampling and training is obviously pertinent to the target use.

If the purpose is to provide help and support a disabled patient, the training will be specialized to select all those brain signals that are relevant to perform the assigned tasks.



Figure 2. Computer and brain activity

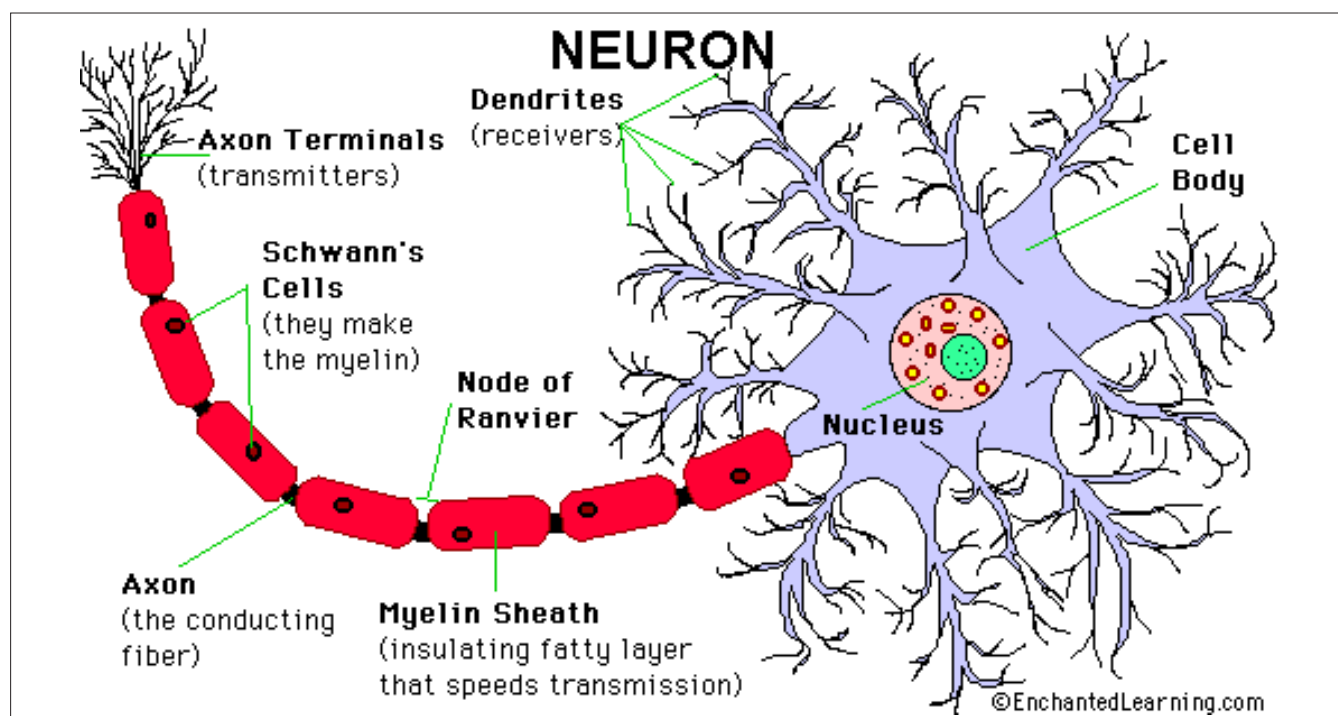


Figure 1. Neuron description



For instance, if the patient needs to move an electronic arm, during the training he will visualize an image or will be asked to think to a specific action attempting to move the electronic arms as it would be his arm. The training can be performed over any type or muscular movement, emotions, thinking as well as any other operation that cause a variation in the activity.

The image below (Figure 3) shows a voltage variation stimulated from a specific event. We can see the difference between the target stimulus and the non-target stimulus demonstrating how BCI distinguish correctly among signals.

Using a commercial BCI system produced by Emotiv or NeuroSky, we can have transfer rates around 5–25 b/min. Greater speed and accuracy may depend on translation algorithms, signal processing, and user training.

On the market more sophisticated devices are available, used in Neural Engineering for medical application, i.e.: the *Computed Tomography* (CT) or *Computed Axial Tomography* (CAT) or Positron emission tomography (PET).

Recently, researchers are developing and expanding a branch called “neuroimaging” that seriously dive into “Thought Identifications”. Thus we are now able to reconstruct words, images, entire thought pattern or even to perform “Intentions Prediction” with an accuracy of 60%.

## The experiment

What are potential risks in this scenario? How can this devices and software be abused by malicious?

Emotiv and NeuroSKY provide hardware and software together with a wide variety of applications, SDK kits and API for free testing and development of the products.

The API allows unrestricted access to EEG sampled signal, leaving the door wide open for malice to develop “spy” applications that attempt to capture and misuse user’s brain signal, hence personal sensitive information.

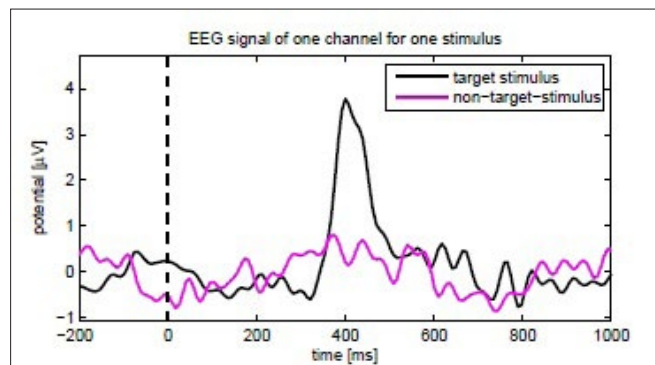


Figure 3. EEG signal of one channel or one stimulus

The experiment performed by the research team from Oxford, Berkeley UCLA and Geneva Universities has proven the feasibility of a side-channel attack using a commercial BCI device.

The test involved 30 “cavy” subjects and consisted of 3 main steps:

- The victim received a verbal explanation of the task by the operator
- Images and messages displayed on screen for 2 seconds to acquire the brain signal sample
- Images being flashed to victims in random order

No specific instructions were given to subjects. The participants had to watch the screen and visualize a sequence of images (Figure 4), such as:

- Pin Code
- Debit Card number
- Geographic Location
- Month of Birth
- Face Recognition – People
- ATM – Bank Information

## Face recognition test

For this test a set of images were displayed for about 2 seconds and 1 of the images was the picture of President Obama. Later another image was displayed on the screen containing the following questions: “Do you recognize any of this people”? Then the images containing people were randomly flashed for the rest of the experiment detecting the brain responses.

The aim of the test was to verify whether would be possible to understand when the participant

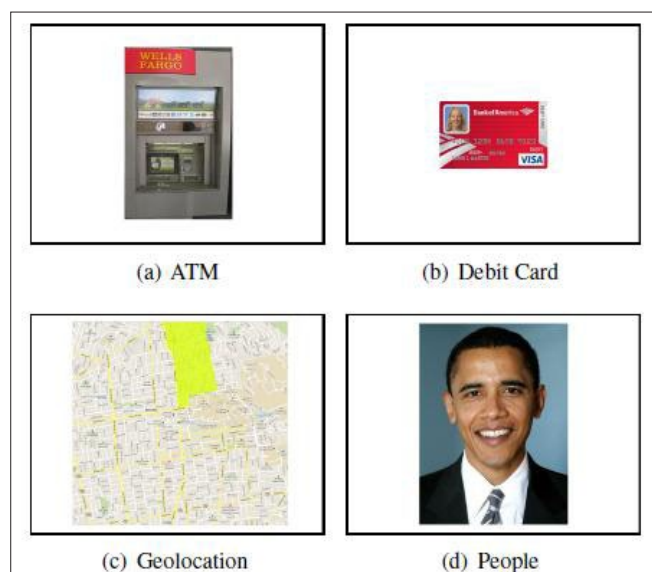


Figure 4. Face Recognition Test

recognizes the image among all the other displayed by reading their EEG responses.

The experiment had a similar procedure for all the other proposed tests. The results of the experiments are visible in the image below (Figure 5)

Obviously, the results of the test must be interpreted in terms of probabilities.

However, the experiment results show a 43% of probabilities of information leakage. This is a very high rate of success also because the researches declared that due to the simplicity of the test, it is possible to assume that a more sophisticated attack may result in a higher successful rate for the attacker.

### The threat Scenario

The assumptions are that:

- BCI devices and EEG techniques will have a rapid progress and dissemination.
- More and more, programmers will develop applications forcing users to map and sample personal sensitive data.

It is not encouraging to admit that methods to steal sensitive data are sadly increasing. There are a number of reasons why personal data is continuously exposed to threats but mainly because it represents an amazing reward for the crime industry.

### Identity Theft – Why IDs are stolen

Identity and personal information are valuable and strictly linked to identity.

Identity theft occurs when an unauthorized person obtains key pieces of personal information about you, such as your Social Security or driver's license number, and uses them to impersonate you. The information can be used to obtain credit, merchandise, and services in your name, or to provide false identification to police, creating a criminal record or leaving outstanding arrest warrants in your name.

We can categorize Identity theft in two ways:

- *Real ID* – i.e.: Thief uses stolen or cloned documents, such as passport or driving license to open new accounts, or use it to impersonate the victims during malicious activities.
- *Cyber ID* – i.e.: The imposter uses a cyber-ID to gain access to an existing account/service, or to create new accounts.

These types of malicious cyber activities may fall under crime such as:

- Unauthorized Use of Personal Identifying Information
- Unauthorized Access to Computer Material
- Unauthorized Access to Computer systems with intent to commit another offense
- Unauthorized Modification of Computer Material

In certain cases stealing a Real ID allows an attacker to gain access to cyber services or use it for online credibility. (id est: Passport ID used to buy flight tickets, ID cards to open online accounts or as evidence to provide when requested from online services)

### What they Steal

Some of the “most wanted” personal information categories are:

- Financial
- Personal Identity
- Criminal
- Medical
- Education

### How they Steal IDs

There are a number of techniques to steal personal data. Here is a list of the most common techniques to obtain personal information:

- Dumpster diving – practically the thief rummages in rubbish and trash bins for identity
- Retrieving data from any kind of devices with storage/memory capabilities including mobile and portable devices.
- Pick-pocketing, housebreaking or mail theft to steal public records such as: bank or credit cards, identification cards, passports, authentication tokens
- Using generic questioning templates. (Real and Cyber information theft)
- Skimming bank cards and creating clone cards. Skimming techniques make use of devices capable of reading magnetic band and integrated chips.
- RFID copy and cloning using contactless devices to copy data.
- Shoulder Surfing or any the observation technique that allow to capture passwords or other type of sensitive information.
- Malicious code, Virus, malware, spyware etc. or any other type of malicious code and technique such as keystroke logging and hidden remote control.
- OS, Application and databases hacking (included hardware embedded firmware) to

## Appendix 1

- <http://techcrunch.com/2012/08/27/brain-hacking-scientists-extract-personal-secrets-with-commercial-hardware/>
- <http://blogs.computerworld.com/cybercrime-and-hacking/20900/hacking-mind-3-new-brain-hacks-expose-new-realm-security-privacy-risks>
- <https://www.usenix.org/conference/usenixsecurity12/feasibility-side-channel-attacks-brain-computer-interfaces>
- <http://www.ocf.berkeley.edu/~anandk/neuro/bci-vertex-abstract.pdf>
- <http://sti.epfl.ch/page-1749-en.html>
- [http://en.wikipedia.org/wiki/Thought\\_identification](http://en.wikipedia.org/wiki/Thought_identification)
- <http://en.wikipedia.org/wiki/Neuroimaging>

retrieve large quantity of personal data, as well as to grant access and abusing privileged accounts of users.

- Brute-force techniques to gain access break ciphers and encryption.
- Fake Advertisement offering bogus jobs or other type of services in order to accumulate resumes and applications typically disclosing applicants' names, home and email addresses, telephone numbers and sometimes their banking details.
- Phishing or scamming through Emails, SMS text messages, phone calls or other forms of communication in order to dupe victims into disclosing their personal information or login credentials, typically on a fake corporate website or data collection form. Spamming can also be vehicle of malware / spyware or so.
- Biometric falsification such as fingerprint identification/theft. Biometric identification methods are recently increasing. Facial reconditioning or retina scanning and other types of methods maybe subjected to complex theft mechanisms in the near future.
- Internet and Social network browsing and be-friending, to obtain personal details published by users as well as for pictures used to create fake identification documents.
- Network attacks such as Man in the Middle or session hijacking to capture inbound and outbound traffic from a computer and obtain sensitive information. The list of the methods used from a malicious to steals personal ID and information has now a new entry.
- ID theft using brainwave samples used for BCI devices.

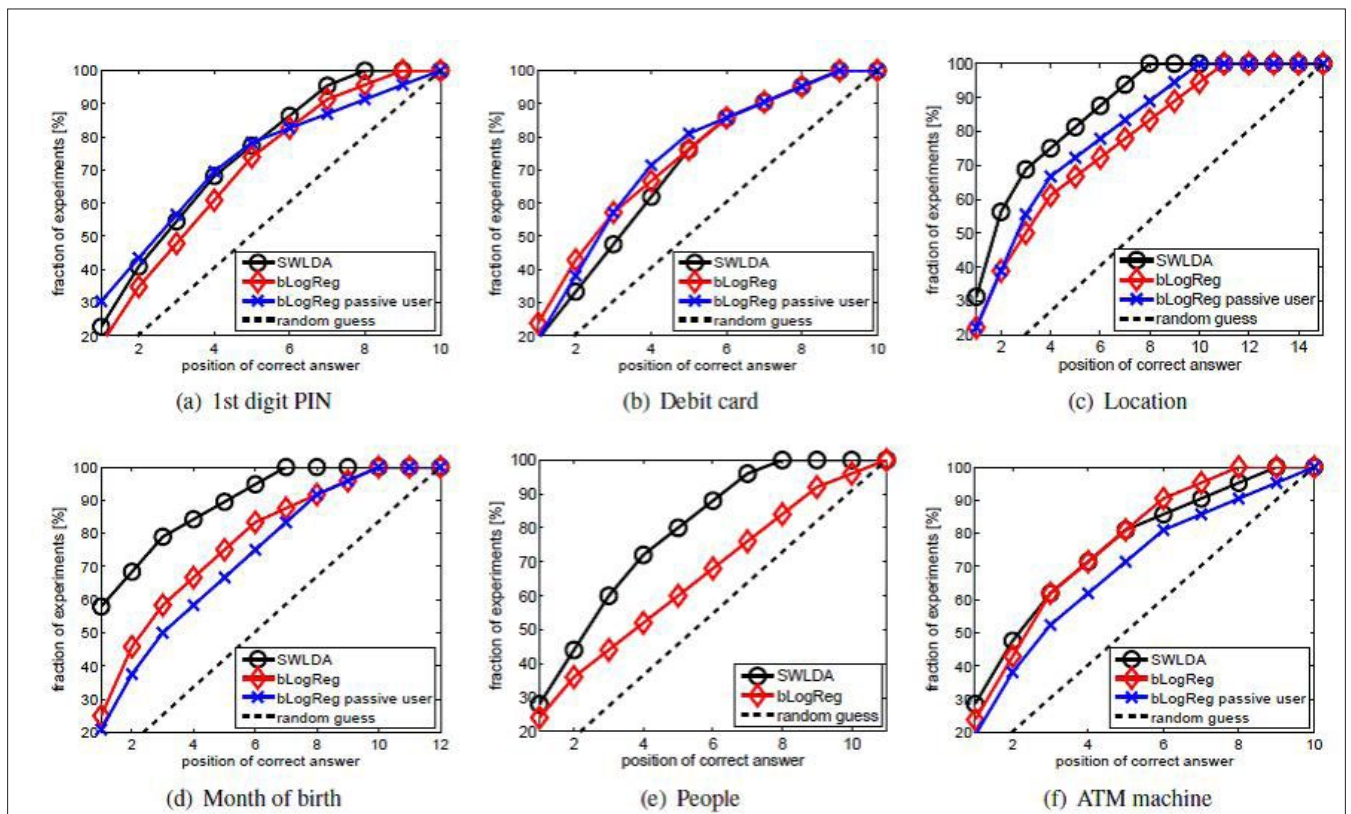


Figure 5. Results of experiments



## Conclusions

As we have seen all these began around 1960, highly supported by US Military. Therefore, the question that spontaneously pops up is: "Why did the USA's Department of Defense spend money on a project that was supposed to improve the living conditions of people affected by neural and physical deficiencies?" Think about it.

Progress can't be stopped but at same time new research are sometimes opening to ethical paradox and moral dilemmas. For the first time, we are aware that we may be very close to achieve Mind Reading in a scientific way. We are likely to shed light on one of the darkest places in the universe and everything we know. Our secrets and past memories may be at risk.

Who will decide on the ethical implication of such powerful tools?

Who will protect us from inappropriate usage and limit potential misuses?

How can we establish standards to ensure human right are preserved, when the last bastion of privacy has fallen?

At the moment we are only able to detect and map brain activity by "reading" the electric movement, but in the near future with the help of technology progress, we may be able to interact with the brainwaves and presumably to "write" into our brain, mimicking sampled patterns and possibly modifying recorded information, hence modifying our personal information and memory.

This would result in more serious risks that may lead to tragic consequence, such as:

- Mind manipulation – by injecting manipulated patterns in our brain.
- Personality mutations – as repercussions on the above threat.
- Memory modification – by overwriting existing memorized information.

Is The Matrix few years away?

---

**SEMBIANTE MASSIMILIANO**

*IT Sec&Risk Eng. at UBS Bank*

*M.Sc. Computer Security*

*Can be reached at: [msembiante@rifec.com](mailto:msembiante@rifec.com)*



# Identity

## information theft and web applications

Identity theft is a process and, like any other process, needs a place to begin. For example, once the smallest amount of personal data is compromised, the next step an attacker can do is test for password or secret questions reuse. This could potentially open up more doors into email accounts, social network sites and much more.

### What you will learn...

- The importance of securing web applications and identity information
- How the smallest vulnerability in a web application can lead to the largest identity information breach
- Security tips for database administration of CMS users
- Several web attack methods of hackers who target your data
- Things to never do with Identity information access

### What you should know...

- General functionality of web applications
- Cross site scripting (XSS)
- Introductory database administration

A majority of people from studies, easily found using Google, reuse passwords. Some of these passwords are reused even from their bank accounts. Some people will use a password “scheme” in which they have an identifier intrinsic to the website in which they log into. Listing 1 is a simple example using Gmail and Facebook.

Can you tell which password is used for which site? g(mai)L – f(aceboo)K

Passwords and their corresponding usernames or email addresses are being dumped on a daily basis to popular pasting websites from hacker groups around the world. Most of which usually come from either SQL injection, or even spear phishing attacks on organizations. What’s even scarier is that a lot of successful, large-scale attacks on companies that reveal all of their customer’s identity information aren’t made public by many hackers. This will leak the data and allow others to steal identities long before the victims, including the organization and their employees, know about it.

What is identity information? This information can include: *addresses, custom secret questions and answers, usernames, email addresses, phone numbers, employee information* and much, much

more. For an organization to keep track of their customers or followers, it has become a very popular practice to employ some sort of web application for record keeping and reporting. A web application is any application in which we can manipulate data using only a web browser. Usually written in a web programming language such as PHP, ASP, Ruby, Coldfusion and supplemental Javascript code, a web application can connect to a databases, write to files, or even call other API’s to access other applications or data outside of the organization.

Some organizations allow outside access to their web applications for their employees from anywhere in the world. *This should never be allowed.* Web applications which can read and write customer identity information to databases should be privately kept behind firewalls. If an organization must allow remote access to a web application to it’s employees, a good practice would be to re-

#### Listing 1. A simple password scheme

```
mypass2012_gL
mypass2012_fK
```

quire that employee to connect to the domain via an encrypted VPN connection. The reason for this is that, no matter which programming language an organization uses, no matter how much they test the software, bugs can present that allow an attacker full access to all database information from anywhere in the world.

*It is extremely easy to accidentally write semantic or logic errors into web code that could give an attacker complete control over all customer identity information.*

Once the personal information is compromised, the attacker becomes one step closer to full identity theft of potentially thousands of victims.

Let's imagine our customers information locked in a safe in which only one guard has a key. The bank is then locked up and an authenticator is standing at the front door of the bank which relays information from customers outside to the guard and then back to the customers. The authenticator has a specific set of rules and instructions in place by the programmer and the guard trusts them but doesn't know what they are specifically. In the case of SQL injection, the authenticator gets compromised and loses all control of these rules and since the guard on the inside of the bank in front of the safe already trusts the authenticator, he gladly gives the customer information to the authenticator who then passes it to the attacker outside.

Now, if we make our application only available to our internal network, we block off the front door of the bank to the world, but open another inside just for us. This helps us in our mission to keep the customers identity information safe but doesn't fully protect it alone. Most of the machines internally can have access to the internet, be compromised, and act as gateways for an attacker to the internal network.

Another thing to consider, is that an institution could use the same "schema" or authenticator for many web applications or web sites. *This should never be done.* If an SQL injection point is found

on their web site, access can reveal not only the web content, but internal customer identity information as well. Some "hosting" websites, will allow one content management system (CMS) user to access all databases for all of the hosted web sites for all companies. This includes any web application software written by their customers! This is extremely devastating to happen.

Our next attack on the web application involves the spear phisher. If an attacker can find even the simplest cross-site scripting (XSS), vulnerability, he or she can then send a malicious link to the web application users. The URL could contain a link to evil javascript code, which rewrites the web page objects, changing the login forms and even sending cookies across the web.

Another way to gain access to databases is by stumbling upon the web application's source code on a compromised system. If our service software is out of date and a known remote exploit exists for one of our services, we could be leaving an even bigger door open to our customer's data. We could also gain access to these files via remote or local file inclusion attacks. The source code of interpreted web languages like PHP is in plain text. This means that our username and password of our web application is just sitting in a file on our server. Listing 2 shows how PHP can connect to a MySQL database.

Now if the attacker did a simple search with `grep` on UNIX/GNU, or `find` on Windows systems, for "mysql\_connect", access could be just one more step away. Sometimes the password is stored in an include file and assigned to a variable. For most other languages, the attacker can just search for the case-insensitive string "password".

If a *local file inclusion* (LFI) attack exists, an attacker can take advantage of the fact that the web server UID can read and write to the server logs. After some digging, the attacker can find these logs, alter his browser's user agent to include interpreted code and then call the file with the browser to run the user agent code. Then all SQL commands can either be ran directly from the browser's user agent string, or from an uploaded shell-like application, giving him or her complete access to the customer information in our databases.

For an attacker to find these web applications and sometimes even their vulnerabilities, he or she has several options. Google as a search engine violently spiders the internet crawling through pages and links within. A special Google search string called a "dork" can be used to find usernames, email addresses, passwords, vulnerable network devices, and anything else from within a site in-

#### **Listing 2.** MySQL PHP Function to connect to a database

```
mysql_connect (where, username, password) ;
```

#### **Listing 3.** Google dork for poor PHP syntax

```
"Warning: mysql_query()" "invalid query"  
site:victimloser2012.com
```



cluding specific file types and any internet accessible web application. For example, Listing 3 will search for a MySQL vulnerability only within the site “victimloser2012.com”

This can reveal the information found in Listing 4. which is very useful to the attacker. Another method is pure brute force. In this method, the attacker creates a simple script that tests an HTTP connection for each word in a list to check for 200 OK status codes. This can find tarball, zip files of backups, text, test, and developmental files that the web application programmer may create during development. A backup file can be downloaded without rendering and the source code can be extracted and read locally revealing passwords for our customer identity information. This method could also return directory traversal vulnerabilities. Sometimes a web server can be configured to allow the public to view the contents of a directory in which no index file resides. This can also reveal files that an attacker can download and view locally (Listing 5).

Listing 4 shows a simple Bash shell script that will test if the HTTP response from curl returns an “HTTP 200 OK” status in the headers. This is done by passing a filename to the application.

#### Listing 4. MySQL Error from poor PHP syntax

```
Warning: mysql_query(): supplied argument
        is not a valid MySQL-Link
        resource
in/directory/webapplications/accounting/
        login.php on line 188
Invalid query: Access denied for user:
        'adminuser2@10.0.13.37'
        (Using password: YES)
```

#### Listing 5. A simple Bash script brute force method for finding hidden files on a web server

```
#!/usr/local/bin/bash
function get {
    if [ "$(curl $URL -sIN | grep OK)" ]
    then echo "$URL is good."
    fi
}
function url {
    URL=http://weaknetlabs.com/$1
    get
}
url $1/
url $1.tar.gz
```

If not the headers from the HTTP response from weaknetlabs.com returns a 404, then the directory or gzipped tarball doesn't exist.

We can also pass a line by line dictionary file to the script that contains lines like “files” and “back-up” using cat and xargs like so:

```
[trevelyn@shell ~]$ cat words.txt | xargs -I {}
        ./getscript.sh {}
http://weaknetlabs.com/main/ is good.
http://weaknetlabs.com/linux/ is good.
http://weaknetlabs.com/linux.tar.gz is good.
[trevelyn@shell ~]$
```

An astounding amount of identity information can be compromised from the result of one simple vulnerability found in an organization's web application.

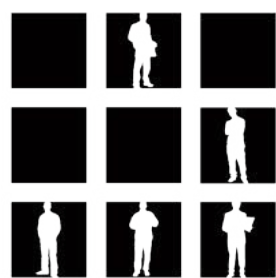
## Points to remember

- Although parallel computing has made it slightly easier for an attacker to decrypt passwords, we should *never* store all customer identity information in plain text. This includes answers to secret questions and passwords. They don't need to be in plain text in the database. We can hash their input and match that against what they have already stored with our data to verify their identity.
- We need to keep our software up to date for our servers and never stop testing our code for vulnerabilities. If we really care about the security of our customer's identity information then let our companies spend money on security. This includes trained professionals in debugging and penetration testing our softwares.
- Never allow direct internet access to our web applications or databases.
- We should never leave backup files anywhere accessible via the web.
- Never use the same schema for our databases for every user or client which plans on hosting customer information and remember to employ multi step validation processes when applicable. Sending a user a text message with a security code is a much better practice than simply asking what their favorite color is.

## DOUGLAS BERDEAUX

*Douglas Berdeaux is a certified wireless security professional and founder of WeakNet Laboratories. His coding includes WEAKERTH4N Linux, WiFiCake-ng, pWeb – Web Application Security Testing Suite, and several Android applications. He currently is a senior web programmer for Duquesne University in Pittsburgh, PA, USA.*





# HACKTIVITY

The IT Security Festival in Central and Eastern Europe  
October 12-13, 2012. MOM Cultural Center, Budapest

**THE LARGEST IT SECURITY FESTIVAL IN CENTRAL AND EASTERN EUROPE  
WILL BE HELD AGAIN!** Real festival mood, presentations, workshops, games, hardware hacking, lockpicking, big friday party and 1000+ hackers from all over the world!!!

Keynote Speaker:

**Jeff Bardin, USA**

Jeff is the Chief Intelligence Officer for Treadstone 71. In 2007, he was awarded the RSA Conference award for Excellence in the Field of Security Practices. He is the most respected expert in the field of cyber crime, cyber terrorism, cyber intelligence.

This talk covers the cyber intelligence lifecycle including examples of denial and deception. Open source intelligence (OSINT) is a critical aspect of asymmetric cyber warfare. It is part of the mosaic defense and one practiced as a method of unrestricted warfare. Methods of cyber espionage, sock puppet creation, infiltration, data collection and analysis are covered. Case studies on creating your own personas while using OSINT tools will be discussed.

...and who can you look forward to?

**ZOLTÁN BALÁZS / HUNGARY** --- Zombie browsers, spiced with rootkit extensions

**ALEXANDER POLJAKOV / RUSSIA** --- Top 10 SAP vulnerabilities and attacks

**JOE MCCRAY / USA** --- The Evolution of Pentesting High Security Environments

**ANDRÁS KABAI / HUNGARY** --- Hunting and exploiting bugs in kernel drivers

**ALEXANDER KORNBURST / GERMANY** --- Self Defending Database

**VIVEK RAMACHANDRAN / INDIA** --- Malicious Wi-Fi Routers for Fun and Profit

**MIROSLAV STAMPAR / CROATIA** --- Spot the Web Vulnerability

**BOLDIZSÁR BENCSÁTH / HUNGARY** --- Duqu, Flame, Gauss malware analysis experiences

**SHAY CHEN / ISRAEL** --- Diviner the new OWASP ZAP extension

**PAYPASS VULNERABILITIES**

**HSRP INSECURITIES**

**„CHIP-TWEET”**

**TRACING MOBILE PHONES**

**ALTERNATIVE USAGE OF PKI DEVICES**

**LOCKPICKING 2.0**

**ALTERNATIVE INTERNET**

**USB = UNIVERSAL SECURITY BUG**

**iOS SECURITY**

**ANDROID SECURITY**

**NAT ATTACK**

**BROWSER BASED ATTACKS**

**DIGIPASS INSTRUMENTATION**

**SECURITY CODE REVIEW**

**GEEK GIRLS**

**ELITE SOCIAL NETWORKS CROOKS**

**AV INSECURITIES**

**AND WHAT ELSE?!**

**Hello Workshops.** Jump from theory to practice: **Hello Injection Hello CA Hello Code Review**

Hardware hacking / Lockpicking (non-destructive/lock-opening) workshop and Urban Warrior competition / **24 hours - Hacker road reloaded.** Get prepared. Never experienced any similar game. Form a team, with a good hacker, a good lockpicker, a good social engineer.

**Tickets are available until 20th of September with 10% discount on [www.hacktivity.com](http://www.hacktivity.com)**

**Full price for adults: 68 EUR / for companies: 150 EUR / Cheap hotels offering also there!**

**Special packages:**

**2 days ticket & 2 nights in a hotel\*\*\* 199 EUR**

**2 days ticket & 2 nights in a hotel\*\*\*\* 299 EUR**

**[packages.hacktivity.com](http://packages.hacktivity.com)**

Sponsors:

Further information and registration: [www.hacktivity.com](http://www.hacktivity.com)

**Deloitte.**

**THINK VALUE.**

**biztributor**

**WEB SHARK**

**ARUBA  
networks**

**ADNOVUM**

**FORTINET.**

**HAKING  
All About IT Security**

**asc  
Safe IT**

# The Hidden Facts About Online ID Theft

Have you ever wondered what is ID, what is behind this word? Do you know what makes the difference between ID and Online ID?

---

## What you will learn...

- what is ID and Online ID;
  - the ways you could lose your Online ID;
  - what are the risks and possible consequences of lost of your Online ID;
  - how to protect yourselves.
- 

## What you should know...

- there are no specific technical terminology, but some basic knowledge about what is risk, encryption, would be nice;
- 

**W**hat is ID? Well, this is something which ultimately identifies you. It doesn't matter how. The obvious answer could be a passport, ID card, *National Identification Number*, *Social Security Number* (SSN). But there are some not so obvious ways for identification. You should think about everything else which could be used like the combination of phone number and address, your birthplace, date of birth. A typical Online ID consists of Username and Password. But it could be also different types of tokens, SIM cards, PIN codes. Sometimes, even the public IP address of your computer or router could be used as your identification.

How it is different from the well known "regular" ID theft? Your proof of ID is something tangible, something you can touch and see. Your Online ID is something virtual. It doesn't exist in the real world. It is stored on some server, somewhere. You cannot touch it. In most of the cases, you don't even know in which country the server is located. When you register with some site, you typically, provide some personal information such as name, e-mail, phone number, address, job title. If the site is related to some purchase, you could also provide information about your bank account, credit or debit card information. In case the account is compromised all or part of the information could be lost as well.

Why your Online ID is interesting to someone? There are many reasons why your ID is interesting to

the bad guys. Finances are the most obvious – they could transfer money from your bank account, they could buy something using your credit card information, they could even borrow money from a bank on your behalf. But there are some not obvious, which could have even greater negative impact to you like reputational, fraud, cheating on your behalf, even revenge. With the growing usage of Internet and online services, your data becomes more and more of a target to organized crime. Once stolen, it could be sold to a wide range of companies.

There are mainly two ways of compromising an identity. The first one is to steal the data from the operator or from the provider of the online services.

Typically the data, which contains information about your ID is stored in some kind of database. How well is this database protected? This is probably, the hardest way for someone to steal your ID. However it is the most efficient. With a single "strike" a hacker could steal thousands and thousands of Online IDs. While in the past such an action was just a question of pride, nowadays the data is sold to different companies. The target of such kind of attacks is the company, not a single person.

The second way is to steal the data directly from you. They would not normally steal your Online ID directly from you. Instead, your account would be compromised. Phishing (or its subtype vishing) is a



typical example. Another way is using non-trusted sites – torrents, key-generators, illegal game sites. When you try to download illegal software or connect (Figure 1) to an illegal game site, you provide information about your ID to a company or person you don't know. There is a big chance the company will sell this information. Of course, there are some not so obvious ways to have your Online ID compromised like sending e-mail to a wrong recipient, easily guessed answers to Secret questions, using unprotected connections.

Another example would be the usage of wireless router (Figure 2) without or with minimal protection. In this case a bad guy could use your unprotected device in order to connect to Internet. Then he could do virtually everything like scanning a server, attack and steal government information, post information to a blog. And the source of all these actions would be your public IP address. Once the attack is discovered, can you guess what will be the first steps of the police – they will first knock on your door.

What are the risks associated with losing your Online IS? They are quite the same as the risks associated with your normal ID: for example someone could use your Online ID to borrow money from a bank, acquire credit card with your name on it or he could buy something expensive on your behalf. But your ID could be also used to write in a blog on your behalf, to make a bomb treat, to threaten the president. And with the growing number of Internet sites and your registrations, the probability of your Online ID being lost is becoming bigger and bigger.

Why it is harder to prevent? Unlike your ID card, the Online ID is something you cannot touch. If you lose your ID card, you will most probably this notice immediately. But if your Online ID is stolen, you may even not notice at all. People are still not used to protect their Online IDs in at least the same way as they are used to protect their ID. They don't

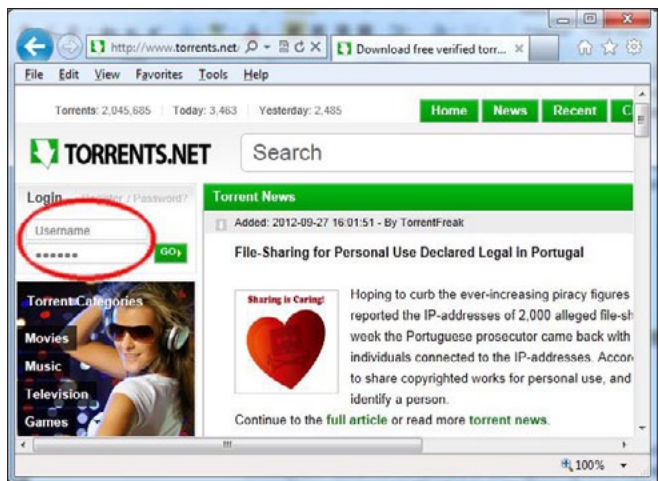
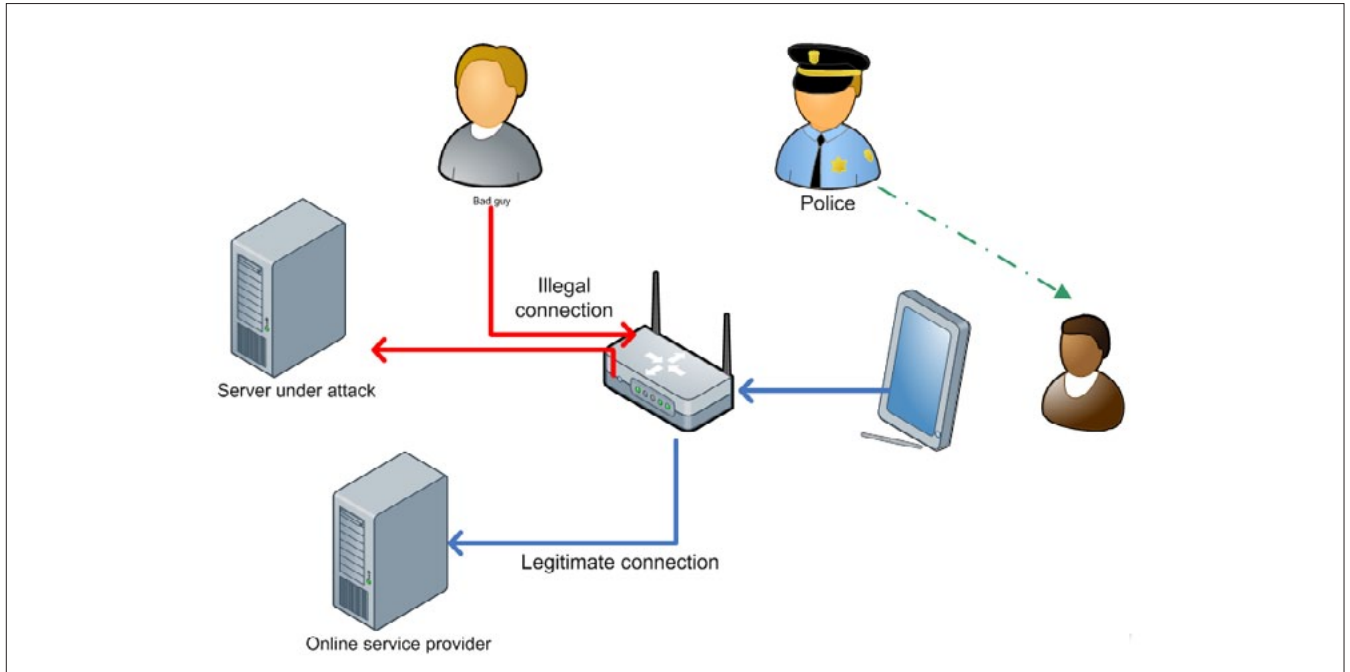


Figure 1. Login to untrusted site

An advertisement for Hakin9. At the top, a man's face is visible, wearing a black bowler hat. Below this is a collage of newspaper clippings, including one from 'The Wall Street Journal' dated 10/27/05, which discusses security developments at Chrysalis-ITS. The main headline of the advertisement is 'Hakin9' in a large, bold, stylized font. Below the headline, it says 'Join our Exclusive and Pro club and get:'. The list of benefits includes: 'Hakin9 one year subscription', 'Full page advertisement in Hakin9 every month!', and 'Information about your company send to over 100,000 Hakin9 readers!'.

More information at  
**en@hakin9.org**



**Figure 2.** Usage of unprotected wireless router

realize the consequences of providing personal information to non-trusted parties. On top of everything, the protection of your Online ID doesn't depend entirely on yourselves. The online service providers are also heavily involved.

What measure could be taken in order to mitigate the risks? There are some simple measures, which will reduce considerably the probability of your Online ID being stolen:

- Provide your data only to trusted parties. Always try to do some basic investigation about the company you are registering with, especially if money transactions are required. Don't underestimate companies with simple registration process. Maybe it is just a free news site where you only read information. But in many cases these sites are not so well protected as the transactional sites. And in case we use the same password for both sites, losing the password becomes far bigger problem.
- Protect your online credentials, never disclose you passwords/PIN, be very careful about phishing sites. Not a single company will ask you for your password/PIN or other credential. They have the proper tools in place and they would reset your password instead of asking you. Only a bad guy would be interested in your credentials
- Close and if possible delete accounts which are not used anymore. Inactive accounts are normally not so well protected as the active ones.

## On the Web

- <http://www.isaca.org/>
- <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>
- <http://www.idtheft.gov/>
- <http://www.idtheft.co.uk/>

- Check regularly your bank accounts and your statements for unusual transactions

What to do in case you notice your ID has been used inappropriately? Besides all other actions, you should remember one more thing – the Online ID theft is a crime in the same way every other theft is. You should report it to the respective legal enforcement organizations.

## Summary

Never underestimate the importance of your Online ID. As already mentioned, even the revealing your credentials for the most unimportant application could become a problem. Remember that the bigger is the number of the online services you use, the bigger is the risk of losing your online ID. On the other hand, the bigger is the number of the service providers, the bigger is the attacking vector for the bad guys.

## DELYAN BOYCHEV

*The author has been working as an Information security manager for a large financial institution since 2002. He was involved in the overall process of protecting the company's data as well as the customer's data, including personal identifiable information.*



[ GEEKED AT BIRTH. ]

[ IT'S IN YOUR PULSE. ]

**LEARN:**

Advancing Computer Science  
Artificial Life Programming  
Digital Media  
Digital Video  
Enterprise Software Development  
Game Art and Animation  
Game Design  
Game Programming  
Human-Computer Interaction  
Network Engineering

Network Security  
Open Source Technologies  
Robotics and Embedded Systems  
Serious Game and Simulation  
Strategic Technology Development  
Technology Forensics  
Technology Product Design  
Technology Studies  
Virtual Modeling and Design  
Web and Social Media Technologies



**You can talk the talk.  
Can you walk the walk?**

**[www.uat.edu](http://www.uat.edu) > 877.UAT.GEEK**

PLEASE SEE [WWW.UAT.EDU/FASTFACTS](http://WWW.UAT.EDU/FASTFACTS) FOR THE LATEST INFORMATION ABOUT DEGREE PROGRAM PERFORMANCE, PLACEMENT AND COSTS.



# Identity Theft:

## Stay Alert, Be Suspicious

Disclosure: This article is not intended to teach you what identity theft is or how much it is dangerous. That, you probably already know.

### What you will learn...

- ID theft facts and statistics
- ID threats and vulnerabilities
- The ways of coping and prevention.

### What you should know...

- A comfortable feeling with this article does require light technical background.
- Information Security orientation can always be helpful.
- No pre-knowledge or working experience in cyber-crime is needed. Mostly important is the desire to be aware.

However, ask yourself if you take the proper precautions, especially when it limits your comfortability and your workflow. Yes, we are all smart people and some of us are professional IT personnel, but here is another question: How many people are you familiar with (could be family, friends or colleagues from work) who were victims of identity theft? Careful, this is a tricky question since the answer is: You cannot know.

### What are we up against

Let's start at the end of a familiar story: An anonymous man contacts your bank representative, identifies himself with your name and ID number and after a brief small talk, asks to transfer a large

amount of money from your investment portfolio, to a different account in another bank.

How could this happen? What went wrong here? How come the thief knew all these secret details and more disturbing is, what further personal information is in the thief's possession? This is a bad end to the story, but unfortunately its beginning was not so good either.

Identity theft also referred to as Identity Fraud or Impersonation, is a sophisticated crime carried out by the action of impersonating to someone else and making actions (mostly financial transactions) on his behalf. It is one of the most popular modern crimes in the 21st century, which victimize millions of people every year worldwide. Despite the intolerable ease

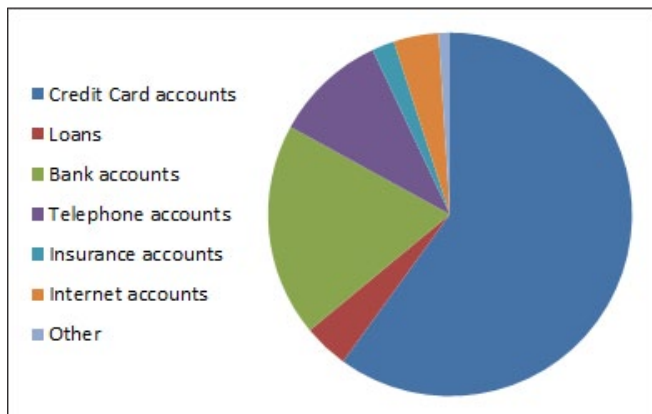


Figure 1. How was stolen information used?

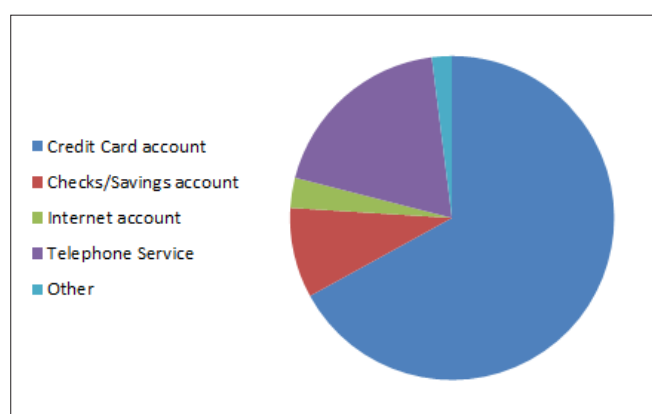


Figure 2. Existing Accounts Misused

with which one can search and find personal information about each and every one of us, taking simple precautions can significantly reduce our chances of being financially or personally damaged.

Back to our story: It is all about access. A successful ID Theft is based on accessibility to one's personal or classified information (ID, Credit Card & Social Security number or even details presented in your Children account on Social Networks). Once an intruder succeeds to find the desired security breach, it can be exploited to get valuable information as a part of the intruder's reconnaissance activity. Next, the intruder will use the victim's information to obtain permissions to databases and financial institutions (websites accounts, bank accounts, credit cards and more ...), withdraw funds from the victim's accounts and purchasing products / services, using the his name and his money.

### Facts & Statistics

The following details have been carefully gathered at the past five years:

- on the *Federal Trade Commission's* (FTC) list of Top Consumer Complaints, identity theft has been the number one complaint for nine years running,
- in the USA, nearly one fifth of all complaints in 2010 were for identity theft,
- one out of four Americans was a victim of ID Theft in the past five years,
- although the number of reported cases of identity theft have slightly decreased in 2011 (relating to the year before) the cost of dealing with these cases has increased considerably, both in terms of time and financial resources,
- 80000 reports have been reported in the UK in year 2011, concerning identity theft,
- the average damage suffering victim of identity theft in the UK is approximately a thousand pounds.

According to the diagrams above (source: *Federal Trade Commission – Identity Theft Survey Report*), the vast majority of id theft reports, indicates the stolen information used for illegal ac-

a d v e r t i s e m e n t



## Web Based CRM & Business Applications for small and medium sized businesses

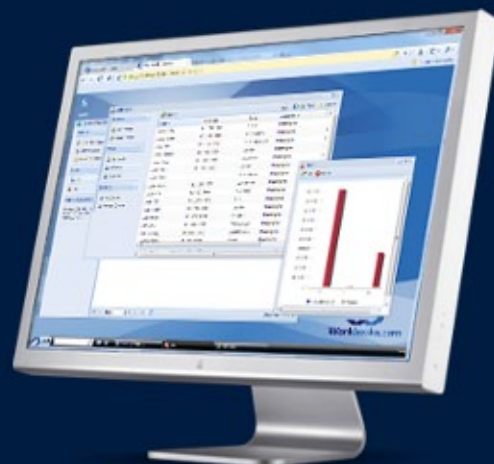
### Find out how Workbooks CRM can help you

- Increase Sales
- Generate more Leads
- Increase Conversion Rates
- Maximise your Marketing ROI
- Improve Customer Retention

### Contact Us to Find Out More

+44(0) 118 3030 100

info@workbooks.com



tivities on credit card accounts (it might suggest a way of prioritize the amount of resources IT personnel should invest for securing information assets). Note that in a significant percentage of cases, the crime is done while actually opening new accounts in the name of the victim.

## Threats Types

There are three major types of identity theft known and common throughout the world. In this chapter I will describe a brief explanation for each type:

- financial Identity Theft,
- medical Identity Theft,
- criminal Identity Theft.

### Financial Identity Theft

In this most common id threat, the intruder will use another's identity to obtain credit, goods and services.

Consequences from financial identity theft include:

- damaged credit,
- credit and debit card fraud,
- savings & Investment account fraud.

### Medical Identity Theft

Medical identity theft occurs when someone uses another's personal information such as insurance

information, to obtain medical services in order to make false claims for medical services or goods.

Consequences from medical identity theft include:

- false medical and pharmaceutical bills,
- false health insurance claims,
- denial different types of insurance claims or coverage.

### Criminal Identity Theft

When a criminal fraudulently use the identity of the innocent victim during the commission of a crime, it is sometimes referred to as Criminal Identity Theft.

Consequences from criminal identity theft include:

- receiving a criminal record,
- obtaining an arrest warrant,
- imprisonment.

## Weaknesses & Vulnerabilities Exploitation

Realization of the threats outlined in the previous chapter is possible by exploiting security breaches and weaknesses. These types of vulnerabilities do not belong only to the "electronic-world" of computing. In many cases, the realization of threats is possible by exploiting physical security weaknesses that exist in our daily habits & behavior.

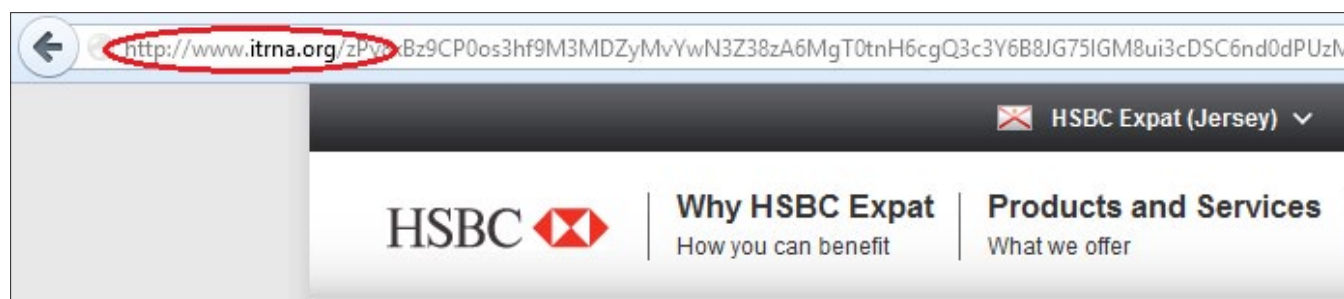


Figure 3. An http URL, addressing for a fake HSBC website

Name	Value	Domain	Size	Path	Expires	HttpOnly	Security
webmailsession	ran@itrna.org:eLPexz	212.199.136.51	92 B	/	Session	HttpOnly	Secure
webmailrelogin	no	212.199.136.51	16 B	/	Session	HttpOnly	Secure
roundcube_sessid	ede6961f46736b0707	212.199.136.51	48 B	/	Session		Secure
Value							
ede6961f46736b07071b769c889898ab							
roundcube_sessauth	Sa0bac8e938b663217	212.199.136.51	59 B	/	Session	HttpOnly	Secure
langedit		212.199.136.51	8 B	/	Session		Secure
lang		212.199.136.51	4 B	/	Session		Secure

Figure 4. 32 digit session-id is stored in a cookie



# CRACK HACK FORUM

CHF is regarded as one of the best online hacking community with over 76k+ members.

CHF was created by a renowned hacker and web specialist named **ProVirus**.

## -CHF-

- CHF has over 2k+ tutorials teaching you the very art of hacking from the very basic to the most advanced level.
- Has a special forum for cracked premium accounts worth thousands of dollars.
- The VIP section is filled with the tools and tutorials unseen elsewhere making the section unique.

Join CHF NOW!!!

[www.CrackHackForum.com](http://www.CrackHackForum.com)

**JOIN  
NOW**

Greetings to: Srinuboy, Terrorbyte, Rain112, Hacker4life, Rynaldo,  
Mschoudhry, fakhrü



In this chapter I will give an example of major security weaknesses (electronic & physical) that could lead to an identity theft.

## Phishing

Phishing is a scam which links to fake site are being sent to the victims. These links are completely identical in content (coded via server-side languages & scripts such as HTML or JS) to the original site and is very similar to its URL address. The Hacker who created this forged website collects the user information of those who try to enter it.

Another method of phishing is a delivery of an innocent-looking email, bearing the details of the victim's bank. Sometimes, the message will report on security problems in the bank and the victim will be asked politely to go to a special site (which he sees as belonging to the bank itself) and enter his username, password & account information online. This method is similar to another theft method called "Social Engineering", which will be discussed later in this chapter (Figure 3).

In the picture above you can see that the URL does not address the original HSBC website ([www. expat.hsbc.com](http://www. expat.hsbc.com)). A user who types in his account details, actually sends his details to the hacker's fake website.

## Pharming

Pharming is a hacker's attack intended to redirect a website's traffic to another bogus site. It can be conducted either by changing the hosts file on a victim's computer, or by exploitation of a vulnerability in DNS server software. Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

## Cookie & Session Theft

Session is being used to identify the user is connected. After signing-in the session-id is marked and accordingly we can identify the user each time the page is loading. If a Hacker finds the

session ID he can easily visit the site by using it. A common way to get the session-id is steal the related cookie using Javascript code injection or XSS attacks.

The Figure 4 describes data from the cookie created following e-mail server connection. The session id is stored inside the field "roundcube\_sessionid". This information could be used by hackers in order to get an access to the mail server, by identifying as the victim.

## Malwares

Malicious software such as Viruses, Trojan horses and Spyware can be used in order to hack the victim's computer, sniff & scan for valuable personal data and then deliver it to the hackers remote machine.

## Social Engineering

Social engineering is a term that describes a non-technical kind of intrusion that relies on human interaction and often involves tricking other people to break normal security procedures. This technique is used in many types of exploits.

Virus writers use social engineering tactics to persuade people to run malware email attachments, phishers use social engineering to convince people to enter sensitive information, and other scammers use social engineering into running software that is useless at best and dangerous at worst.

**READ more about weaknesses and vulnerabilities exploitation in our full issue.**

## RAN LEVI

*The author has been working as an Information Security Consultant & Auditor in a variety of enterprises of all areas of industry, implementing security methods and techniques for the past eight years. The author is also involved in research & developing Bioinformatics algorithms and solutions for Computational Biology problems.*

## Glossary

- cyber-crime (or computer-crime): The Department of Justice categorizes computer crime in three ways: 1) attacking computers of others (computer as a target) 2) using a computer to commit a crime (computer as a weapon) 3) using computers to store illegal or stolen information (computer as an accessory),
- dns servers: DNS servers are computers responsible for resolving Internet names into their real IP addresses,
- identity theft: Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's confidential data in ways that involves fraud or deception typically for economic gain,
- reconnaissance: Any method of scanning and gathering information of an entity in order to profile the target organization or network or even his physical habitat for the efficient attack tactics,
- xss (or Cross-Site-Scripting): is a type of a security breach typically found in Web applications that enables attackers to inject client-side script into Web pages viewed by other users.

# Learn ethical hacking > Become a Pentester™

- ✦ Get trained today through our exclusive 7-months hands-on course.
- ✦ Gain access to our complex LAB environment exploiting vulnerabilities across many platforms.
- ✦ Receive a trainer dedicated to you during the 7 months.
- ✦ 10 different hands-on engagements, 2 different certifications levels.

MONTH 1	<ul style="list-style-type: none"><li>&gt; Vulnerability Assessment - level 1</li><li>&gt; Vulnerability Assessment - level 2</li><li>&gt; Vulnerability Assessment - level 3</li></ul>
MONTH 2	<ul style="list-style-type: none"><li>&gt; Network Penetration Testing - level 1</li><li>&gt; Network Penetration Testing - level 2</li></ul>
MONTH 3	<ul style="list-style-type: none"><li>&gt; Network Penetration Testing - level 3</li></ul>
MONTH 4	<ul style="list-style-type: none"><li>&gt; Web Application Penetration Testing - level 1</li><li>&gt; Web Application Penetration Testing - level 2</li></ul>
MONTH 5	<ul style="list-style-type: none"><li>&gt; Web Application Penetration Testing - level 3</li></ul>
MONTH 6	<ul style="list-style-type: none"><li>&gt; Certification Exam 1 - Certified Cyber 51 Pentesting Professional - (CC51PP)</li></ul>
MONTH 7	<ul style="list-style-type: none"><li>&gt; Certification Exam 2 - Certified Cyber 51 Pentesting Expert - (CC51PE)</li></ul>

~~Regular Price~~  
1260 USD

**Discounted Price**  
**999 USD**

[Sign Up Now](#)





# How to Secure your

## company's network with the Juniper Netscreen NS Series Security Appliance – Part 1

In last month's article we focused on the Cisco PIX Firewall, a cost effective yet still solid platform in the previously owned market. This month the focus is on a comparable unit from another top tier vendor that is also a great purchase in the enterprise resale market and still provides solid, fast efficient enterprise class stateful inspection at the perimeter with some advanced application layer features. The Juniper Netscreen.

### What you will learn...

- How to cost effectively secure your company's network with enterprise class hardware
- How to operate with the Juniper Netscreen Security Appliance
- Differences and similarities between ScreenOS and PIX IOS

### What you should know...

- Basic knowledge of network security
- General knowledge of network and network security equipment
- Understanding of IP subnetting and TCP and UDP services
- General understanding of NAT/PAT and Access Lists.

Comparable to the PIX 515 model and used in typical branch office, mid sized regional office deployments are the NS 25 NS 50 and NS 204 models which are the comparable model to the 515 series Cisco PIX and 5510 series of the ASA. These models are available via resellers often at incredible savings and still provide solid basic stateful inspection along with some advanced application layer capabilities. The capabilities between the two types of appliances are similar including stateful inspection, transparent layer 2 capability along with some application layer capabilities including acting as VPN tunnel endpoint or client endpoint. But there are some differences in the CLI between the two security operating systems and in how you approach the basic configuration steps.

This article will be presented in two parts so we can cover not only ScreenOS configuration and implementation of the Netscreen but how they relate to the Cisco PIX IOS and PIX/ASA platforms. In this first section we will take a look at the various features of the Netscreen, some basic configuration parameters and security parameters such as "policies" and how they relate to PIX IOS ACL's, Virtual Routers and their purpose as well as some of the various models limitations and features. In part two we'll take a more in-depth look at hard-

ening the Netscreen particularly attack signatures and defensive measures (including a couple of really cool built in signatures not found on the PIX) and some standard branch and regional office deployment scenarios as well as take a closer look at some specific configuration variances and similarities to the PIX IOS.

### Basic ScreenOS Differences from the PIX IOS

There are some differences between the ScreenOS and PIX IOS such as Policies as opposed to ACL's. Rather than using ACL's Screen OS uses policies to assign permissions to interfaces. Rather than NAT, ScreenOS uses MIPS\DIPS (*Mapped and Dynamic Mapped IP's*) but the end result is the same, a registered internet routable IANA address mapped to an internal RFC 1918 private address. We won't go through each and every syntactical difference between the PIX IOS and ScreenOS but we will review some of the more significant structural differences in the configurations between the two. We'll take a brief look at some of these differences in part 1 along with a general overview of the Netscreen and ScreenOS. In Part 2 we'll take a closer look at defense protections and capabilities, attack signatures and defenses, some basic deployment

scenarios where these application layer defenses can be helpful and finally some basic steps to get your Netscreen up and running in a basic web application services deployment and how the configuration examples relate to similar configurations with the PIX IOS.

## ScreenOS Zones

Perhaps the most obvious is the out of the box config. The PIX has gateway functionality out of the box. Interfaces are designated as internal and external (Inside, Outside) with security level assignments preassigned. Lower security level interfaces cannot pass traffic to higher level security interfaces without a specific rule (ACL) but a higher security interface can pass traffic to a lower security interface without a specific rule applied permitting that specific traffic. Rather than security levels the Netscreen uses Zones to accomplish security levels. Default zones are created and interfaces assigned out of the box. On an NS 50 for example, you'd have 3 zones that have interfaces assigned. Trust, Untrust and DMZ, the names being self explanatory.

Trust translates to the Inside interface on the PIX. Untrust to the Outside and of course DMZ to DMZ. However this does not mean traffic can by default go from one interface to another. Traffic between two interfaces assigned to different zones will not pass without a rule applied. Traffic between interfaces within the same zone however can pass without a rule, for any traffic to traverse any interface a specific rule must be applied.

## VRs – Virtual Routers On the Netscreen

One of the somewhat unique features of the Netscreen in comparison to the PIX is the use of virtual routers which can be bound to zones and thus indirectly to interfaces. Virtual routers are referred to in the ScreenOS as “vr” and are bound to zones. Two vr's are created in the ScreenOS by default, one for Trust and one for Untrust, but they are not automatically assigned to the respective zones. You can create additional vr's as needed, such as for multiple routing protocols to multiple ISP's.

The primary purpose for the vr's are to conceal your internal route table from your external interface but they will conceal a routing table from any zone to any zone when those zones are placed in separate vr's. This can be helpful when utilizing routing protocols on the Netscreen. By placing the untrust zone in the untrust-vr and the trust zone in the trust-vr you create two separate route tables separate from the other, concealing the in-

ternal routes to the untrust side of the appliance. This hides routing information from the internal network from the external interface which is particularly of help when routing protocols are implemented.

Naturally on some branch office implementations a single internal subnet might be deployed with the Netscreen acting as a gateway appliance to the ISP. In such implementations the advantages of separating the two are negligible since there's no actual routing going on the internal subnet. Just an interface to a private RFC 1918 subnet. So on most implementations of this type you can keep both default zones (trust – untrust) in the trust-vr for ease of use. On implementations where you decide to separate the zones via a virtual routing table you will need to remember to add routes between the zones otherwise you won't be able to traverse the zones.

To quickly view the configured virtual routers on your Netscreen use the following command;

```
netscreen-> get vr
```

The following is the output from an NS-50 running ScreenOS 5.4

\* indicates default vrrouter

A - AutoExport, R - RIP, O - OSPF, B - BGP, P - PIM

ID	Name	Vsys	Owner	Routes	MRoutes
Flags					
1	untrust-vr	Root	shared	0/max	0/max
* 2	trust-vr	Root	shared	9/max	0/max

The outputs fairly self explanatory however the one significant thing we learn from this output is this Netscreen is configured to only use the one virtual router (trust) for all interfaces. There are 9 routes in the route table comprised of routes from both the DMZ, untrust and trust zones. No other virtual routers have been implemented on this appliance. The other thing we see from this output is both the trust and untrust interfaces as well as any other interfaces configured on the appliance (in this example there is one additional interface acting as a DMZ) are all bound to the trust-vr. Thus if we examine the route tables we'll see that all routes appear in the trust-vr route table and no routes appear in the untrust-vr (Listing 1).

The output again is pretty straight forward (note the get route command. Same command on the PIX IOS except of course for the use of “show” commands as opposed to “get”). IP prefix (the part of the packet the route engine examines), the

Interface, Gateway, Metrics, etc. The Vs is the “virtual system”, which is something we’ll take a look at later on in part 2. The virtual system is however just what it sounds like. In this instance its “root”. The interesting data here of course is again the lack of any routes in the untrust-vr, telling us that all active interfaces on this appliance are assigned to the trust-vr. We also see no OSPF, BGP, EBGp, (etc) routes in the table so it is not as important as if we were using these protocols. Another interesting thing we see here that we don’t see in the PIX IOS, is the support for these routing protocols, another reason to love the Netscreen. The ability to do things like export BGP routes from the untrust-vr and propagate them into the trust-vr greatly expand the enterprise level functionality of the Netscreen.

Standard DMZ Architecture with the Netscreen & Hardware Options

One thing I like about the PIX 515 series is the ability to add up to 4 physical DMZ’s via DMZ modules (either 1 or 4 port). The older smaller NS series Netscreen’s like the NS 25, 50 and 204 come with fixed interfaces and no expansion slots. The larger

models like the 5200 and 5400’s are modular but you’re spending in the thousands and tens of thousands depending on the unit.

Keeping with the “on a budget” approach for the mid sized branch or regional office looking for a solid stateful inspection perimeter appliance with application layer features the Netscreen NS series provides a fantastic bargain in the resale market that still provides solid stateful inspection including DOS, DDOS protection, VPN and Layer 2 capabilities and other advanced features. But it doesn’t provide as many interfaces as the PIX 515 series with a 4 port DMZ expansion card. So if you have the money the SSG140 is a much better selection as it provides more interfaces and of course because it runs the much more desirable ScreenOS 6 and has many more application layer signatures, (200,000+) as well as other advantages, however the average price on these even in the resale market can run a few thousand dollars for a branch office size model (Figure 1).

A more cost effective option if you’re on a strict budget is the End of Life Netscreen NS series units. Of course the NS series are end of life and will not provide the all the features of the newer

Listing 1. Standard DMZ Architecture

```
netscreen-> get route

IPv4 Dest-Routes for <untrust-vr> (0 entries)
-----
H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
iB: IBGP eB: EBGp O: OSPF E1: OSPF external type 1
E2: OSPF external type 2

IPv4 Dest-Routes for <trust-vr> (9 entries)
-----
```

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vs
*	10	0.0.0.0/0	eth3	10.200.1.1	S	20	1	Ro
	6	10.20.1.1/32	eth2	0.0.0.0	H	0	0	Ro
*	4	10.101.10.1/32	eth1	0.0.0.0	H	0	0	Ro
*	2	10.100.1.2/32	eth1	0.0.0.0	H	0	0	Ro
*	1	10.100.1.0/24	eth1	0.0.0.0	C	0	0	Ro
*	3	10.101.10.0/24	eth1	0.0.0.0	C	0	0	Ro
*	7	10.200.1.0/25	eth3	0.0.0.0	C	0	0	Ro
	5	10.20.1.0/24	eth2	0.0.0.0	C	0	0	Ro
*	8	10.200.1.11/32	eth3	0.0.0.0	H	0	0	Ro



SSG models but if you are trying to cut costs and just need an enterprise class firewall capable of protecting your gateway perimeter then the NS Series still offers basic protection with some cool extras. Online auctions usually let them go fairly cheap, between 50 and 100 bucks. But if you want one from a reseller then you'll stay pay a few hundred bucks normally, (or more depending on the reseller). The drawback of course (and why its so cheap) is they only run the older ScreenOS 5.x version whereas the SSG models run the newer more desirable (ScreenOS 6 provides a more feature rich environment and more functions and capabilities) version 6 with many more application layer features including many more attack signatures, AV signatures, etc. But the NS Series are still a solid perimeter device providing stateful inspection, DOS and DDOS and other attack protection as well as being cost effective enough for even the tightest of budgets.

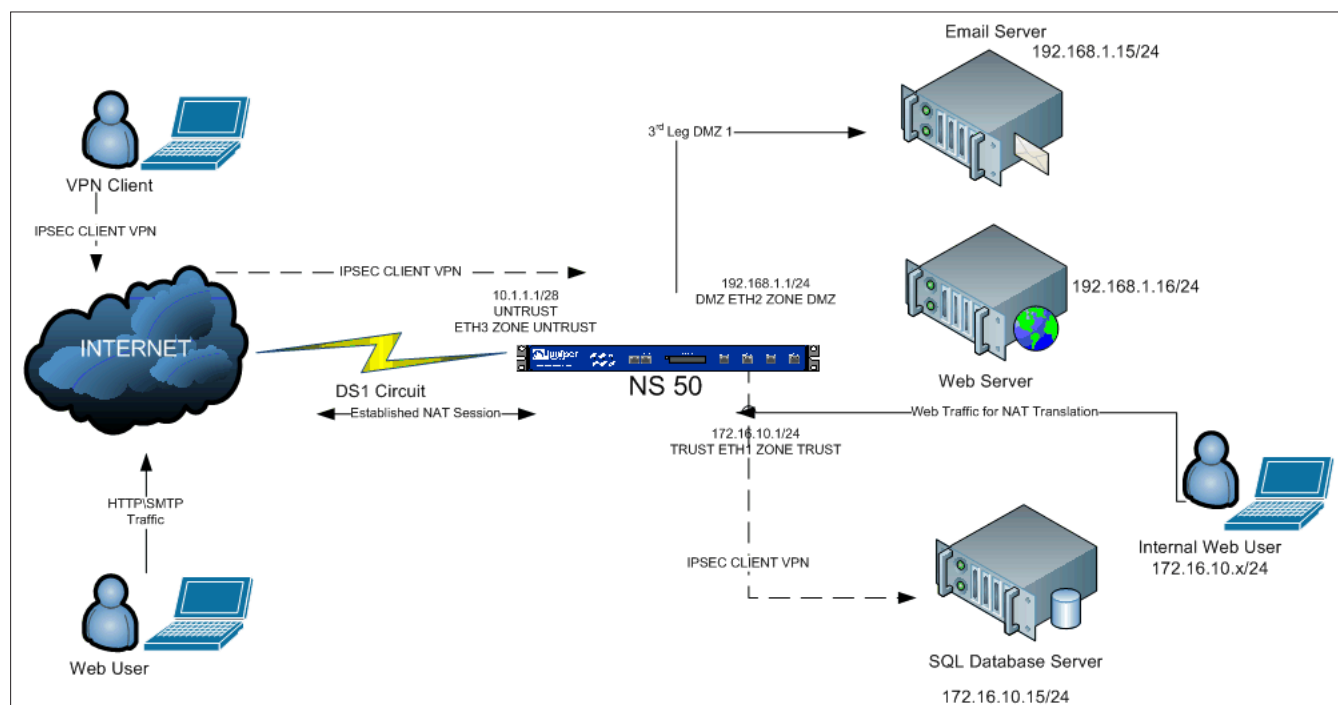
The DMZ interface is usually going to be defined on Ethernet2, and functions similar to the PIX except again, no security levels. So instead of a default traffic pattern traversal being implemented you have to expressly define traffic permissions and direction to enable flow to and from the DMZ, usually to the external or untrust network in a typical branch office deployment. The DMZ will have a private RFC 1918 address assigned in most instances (unless you want to route to the DMZ subnet from the untrust zone) and a MIP assigned to it with a policy pointing to

the MIP as the destination. When the DMZ host sends return egress traffic it will use the MIP address in the same way a host on the DMZ of the PIX uses a static NAT mapping. If you want hosts on the private trust subnet to access hosts on the DMZ subnet you merely need to establish the same type of policy you would for accessing the external untrust zone. We'll take a brief look at policies in the next few sections.

## ScreenOS & Concurrent Sessions

Some networks of course can benefit from the SOHO models of the SSG (like the SSG 20 and Wireless models) but these are for small offices or home offices and again you'll be looking at the same issues if you have more than a few users that we saw on the smaller SOHO PIX models. With Cisco they're referred to as "concurrent connections" but on the Juniper appliance they're known as "sessions but the make up of them are similar. TCP or UDP connections equal a session, so one user with a few web pages, maybe an email client where the server's beyond the SSG, an FTP program or Database app, etc is going to use up a lot of sessions. I've seen 10 users use up as much as several thousand sessions.

The SSG 20 has a maximum session allocation of 8064 sessions which I personally wouldn't use in an office with any more than 5 or 6 users, although theoretically you could have around 20. But ideally you'll want to keep your load well below 85 percent on the firewall. In ScreenOS you can quickly



**Figure 1.** Basic Inside, Outside Deployment with 1 DMZ

determine the number of sessions available and if whether you're having dropped sessions using the following command.

```
netscreen-> get session info
```

The output seen below is the actual output from this command ran on an SSG 20 that was experiencing drops.

```
netscreen-> alloc 2588/max 8064, alloc failed 516,
                mcast alloc 0, di alloc failed 0
total reserved 0, free sessions in shared pool
                5476
```

We quickly see that while currently the allocated sessions are well below the 8064 total available, that the unit has dropped 516 sessions.

This means the appliance is not large enough to support the user base and its time to upgrade to a unit capable of more sessions.

You can also of course control the number of sessions available to users and services but on a smaller network you'll find its more trouble than its worth. Best just upgrade the device to the next size up. Once you take a quick look at all the services running on your network through a protocol analyzer you'll quickly see how just a handful of end users can quickly use up your available sessions (Figure 2).

An SSG 140 provides 48,000 sessions which is comparable to the NS 50 which has a max 64,000 sessions (Depending on the version of ScreenOS you are running. Older versions will have less ses-

sions for the same model) which would be about the right size for 100 to 150 users comfortably. While you can of course have more users I've found that allocating 5000 sessions per 10 users is a good rule of thumb to follow, whether we're talking about Cisco or Juniper. You may find a different ratio works for you depending on your user base and their usage patterns but in general I think most will find that's a good ratio of users to session's if you like happy users and low maintenance. The important thing to remember here is just as it is with the PIX/ASA, users don't directly equate to sessions. Far from it. It is an indirect relationship and a dynamic one based on services and applications being offered and the usage patterns of your users.

## ScreenOS Policies

Security Policies are the ScreenOS equivalent of PIX IOS ACL's (or conduits in older versions) that permit traffic to and from the various interfaces on the Netscreen appliance. Policies allow defined traffic to traverse interfaces in different zones. Policies are at the core very similar to Cisco ACL's.

A policy will define 4 actions;

- Permit
- Deny
- Reject (sends TCP reset)
- Tunnel (encrypts for VPN, either LT2P or IPSEC)

A policy is generally defined by 4 basic parameters.

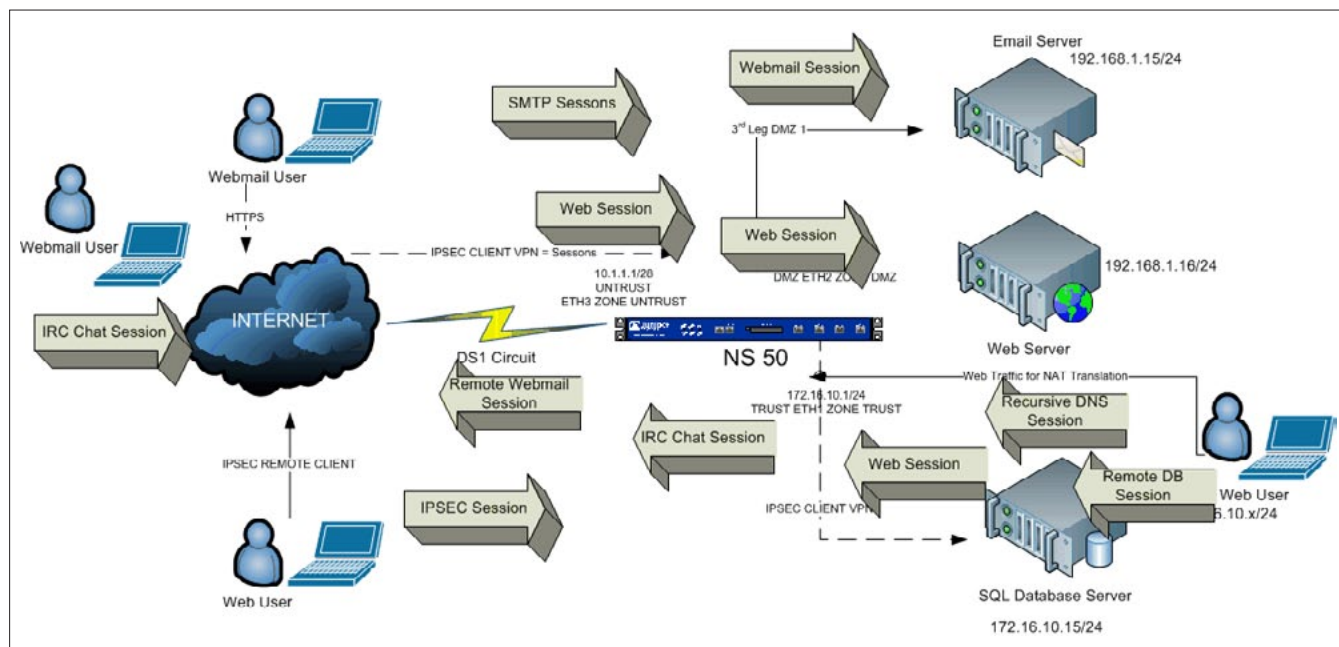


Figure 2. 1 Power user = Multiple Sessions

- Source
- Destination
- Service
- Action

The source will be a network (wire) or host address. Same for the destination (Combined the source and destination define the direction). The Service will be the protocol. Together they make up the socket for the connection. The source and destination of course provide direction and the action defines whether to permit or deny (Or “encrypt” for VPN tunneling). These are the same general types of variables that define a standard Cisco ACL.

The difference between them lies more in their implementation order and syntax, a prime example being the default traffic traversal behavior between interfaces. In the PIX IOS trust traffic is automatically permitted to the untrusted interface once the interfaces are brought up and basic NAT or PAT rules applied. This is due to varying security levels being assigned to the interfaces. The higher the security levels have access to the lower security levels. Lower security levels need ACL's to access the higher security levels. But in ScreenOS interfaces are assigned to security zones but these zones do not have security levels assigned to them by default. Instead total lockout is in effect on any interfaces in different security zones until a policy is assigned. Thus really there is no “outside, inside, DMZ”, etc. The default names are out of convenience and not functional. Without an accompanying security policy defined, no traffic from the “Trust” network can traverse to the “Untrust”. In other words unlike the PIX, the outside isn't automatically outside nor is the inside automatically inside. You have to make them that way. You can't just bring up the interfaces and apply PAT and expect to be surfing the web with the Netscreen. You will need policies defined first.

An example of an outbound policy permitting all traffic from the trust to the dmz zone would look like this.

```
Netscreen->set policy id 1 from "Trust" to
"Untrust" "Any" "Any" "ANY" permit log
Netscreen->set policy id 1
```

The same sort of policy is used to permit traffic to the DMZ zone or for any zone. A common issue with first time Netscreen users who are used to the PIX or other gateway type appliances is to forget to permit traffic in both directions that they

want it to travel. Of course you can be much more specific and define multiple services and parameters.

### The Syntactical Structure of Security Policies compared to PIX/ASA IOS ACLs

ScreenOS security policies are at the end of the day quite similar to PIX IOS Access Lists, and like ACL's are tied to an interface and define a state, either permit or deny. However unlike Cisco ACL's they also define an additional state “encrypt” which is used for VPN encryption. It differs from the application of the Cisco ACL used for VPN encryption by defining encryption in the state whereas PIX IOS simply defines the ACL. In PIX IOS the ACL is not applied to the interface but instead simply defined, then referenced in the Crypto map. But the differences don't stop there at least syntactically. Policies “look” a lot different on the surface from ACL's but they accomplish pretty much the same things when dealing with basic in and out firewall functions.

Let's take a quick look at a PIX IOS ACL compared to a ScreenOS policy. We'll define a simple basic inbound ACL to provide SMTP traffic to a standard mail server and compare it to a ScreenOS policy that defines the same access. For the purposes of this article we'll pretend that 192.168.1.1 (In actuality 10.1.1.5 is an RFC 1918 address however for the purposes of the article we will pretend it's a registered address) is the outside (registered IANA) address and that the internal (RFC 1918) addresses sit on the 10.1.1.0/24 network.

### PIX IOS

```
PIX# access-list 101 extended permit tcp any host
10.1.1.5 eq smtp
access-group 101 in interface outside
```

### ScreenOS

```
netscreen->set policy id 3 from "Untrust" to
"Trust" "Any" "MIP(10.1.1.5)" "SMTP" permit log
netscreen->set policy id 3 application "SMTP"
netscreen->set policy id 3
```

The ACL is pretty straight forward as we can see. The ACL is defined first, then the state (permit in this instance), then the protocol (TCP), the source (any) and the destination (10.1.1.5) and finally the actual protocol (service as Juniper refers to it) is defined, in this case SMTP (SMTP defines the standard TCP port of 25. If another port is in use by your mail server then the actual port



number would be stated in place of the protocol). The Screen OS Policy looks a bit different but accomplishes the same thing. First we see it defines the policy and sets an “ID” to reference it, (3 in this example, similar to the ACL id of 101). Then it defines the source of the traffic (Untrust zone), the destination (Trust zone), the source address (any) and the actual destination address (MIP(MIP defines the mapped IP or NAT'd address in use, in most instances on the untrust zone mapped to a private RFC 1918 address in the trust or dmz zones) (10.1.1.5). We also see that we must specify the service and bind the service application (SMTP) to the policy;

```
"netscreen->set policy id 3 application "SMTP"
```

ScreenOS comes with many services predefined (port numbers already mapped). To see the pre-defined services already installed on your unit use the following command.

```
netscreen-> get service pre-defined
```

The following output is from a live Netscreen NS50 running ScreenOS 5.4 (Listing 2).

The output is truncated for brevity but we see there are a total of 136 predefined services on this unit. And we must define the policy ID. These are

Listing 2. Live Netscreen NS50 running ScreenOS 5.4

```
netscreen-> get service pre-defined
```

Name	Proto	Port	Group	Timeout (min)	Flag
ANY		0	0/65535 other	30	Pre-defined
AOL		6	5190/5194 remote	30	Pre-defined
BGP		6	179 other	30	Pre-defined
CHARGEN		17	19 other	1	Pre-defined
DHCP-Relay		17	67 info seeking	1	Pre-defined
DISCARD		17	9 other	1	Pre-defined
DNS		17	53 info seeking	1	Pre-defined
ECHO		17	7 other	1	Pre-defined
FINGER		6	79 info seeking	30	Pre-defined
FTP		6	21 remote	30	Pre-defined
FTP-Get		6	21 remote	30	Pre-defined
FTP-Put		6	21 remote	30	Pre-defined
GNUTELLA		17	6346/6347 remote	1	Pre-defined
GOPHER		6	70 info seeking	30	Pre-defined
GTP		17	2123 remote	3	Pre-defined
H.323		6	1720 remote	30	Pre-defined
HTTP		6	80 info seeking	5	Pre-defined
HTTP-EXT		6	7001 info seeking	5	Pre-defined
HTTPS		6	443 security	30	Pre-defined
ICMP Address Mask			0/65535 other	30	Pre-defined
ICMP Dest Unreachable		1	0/65535 other	30	Pre-defined
ICMP Address Mask		1	0/65535 other	30	Pre-defined
ICMP Dest Unreachable		1	0/65535 other	30	Pre-defined
ICMP Fragment Needed		1	0/65535 other	30	Pre-defined
ICMP Fragment Reassembly		1	0/65535 other	30	Pre-defined
ICMP Host Unreachable		1	0/65535 other	30	Pre-defined
ICMP Parameter Problem		1	0/65535 other	30	Pre-defined
ICMP Port Unreachable		1	0/65535 other	30	Pre-defined
ICMP Protocol Unreach		1	0/65535 other	30	Pre-defined
ICMP Redirect		1	0/65535 other	30	Pre-defined
Total number of pre-defined services shown: 136					

done as separate commands but are part of the defined policy.

To set a simple rule permitting all internal traffic from the inside to the outside on the Netscreen we would set a policy statement resembling this one (although the ID number can vary)

```
Netscreen->set policy id 1 from "Trust" to
"Untrust" "Any" "Any" "ANY" permit log
Netscreen->set policy id 1
```

## Static NAT & MIPS

NAT and PAT functions including one to one static NAT translations, Dynamic NAT Pools and Port Address Translation aren't much different than they are in the PIX IOS except for the syntax. They look a bit different but accomplish the same thing so we won't spend a lot of time on them in this section. Basic NAT is basic NAT. Later we will look at other features of NAT but in this introduction we'll just look at a typical one to one translation, in this instance permitting traffic from the external interface to a server on the inside. In PIX IOS we define static one to one NAT translations via the "static inside,outside" command. For ScreenOS we'll use the "MIP" (mapped IP) command.

## PIX IOS

```
PIXFIREWALL(config) # static (inside,outside)
10.1.1.5 192.168.1.15 netmask 255.255.255.255
```

This maps a static IP to the internal IP of the mail server sitting on the DMZ, note the 32 bit mask identifying the host, and not the actual subnet mask of the wire.

## ScreenOS

```
NETSCREEN-> set interface "ethernet3" mip
10.1.1.5 host 192.168.1.15 netmask
255.255.255.255 vr "trust-vr"
```

Like the PIX IOS the outside IP is mapped first to the inbound IP, but in this case rather than binding the internal IP to the interface on which it sits it binds the entire process on the outside (ethernet3) interface to the mapping. But it does map it to the virtual router, in this case the trust-vr (remember vr's are used to isolate route tables). Similar to the PIX it uses the 32 bit network mask to define the host.

## Syslogging

One keyword shared with the PIX/ASAACL's is the "log" command at the end, which instructs the appliance to log the when the action defined is met (usually a deny). Identifying the Syslog server is pretty straight forward as well. Like the PIX IOS you define the server IP, port, protocol (TCP or UDP, default is the standard UDP 514), here we set it to TCP for a better guarantee of delivery (Listing 3).

## Vulnerabilities in ScreenOS 5.x

Like the PIX there are some documented vulnerabilities with ScreenOS 5 (and before) however again like the PIX these are able of being mitigated by either upgrading the OS or via work-arounds or configuration options (and omissions).

Only a handful of vulnerabilities are identified by CVE and all of those are not pertinent to versions of ScreenOS above 5.0, therefore we won't spend a lot of time on them other than to look at a few and how they can be easily mitigated or in most cases negated.

## Cross Site Scripting (XSS) Vulnerability (CVE-2008-6096)

Prior to ScreenOS 5.4 (r10) ScreenOS is vulnerable to a cross site scripting attack which allows attackers to inject arbitrary script or HTML into the Username field in both the telnet and web interface login.

### Listing 3. Netscreen

```
Netscreen->set syslog config 192.168.1.10 port 1000
Netscreen->set syslog config 192.168.1.10 log all
Netscreen->set syslog config 192.168.1.10 facilities local0 local0
Netscreen->set syslog config 192.168.1.1.10 transport tcp
Netscreen->set syslog src-interface ethernet1/1 - Sets the interface used to reach the
syslog server
Netscreen->set syslog enable
```

## FIX

The solution to this vulnerability is either upgrade to release 10, or simply don't open HTTP/HTTPS access or Telnet access to the Untrusted side of your Netscreen, which by the way is a no brainer anyway. Opening telnet or http management to your Netscreen from the outside is just a bad way to fly. It is always advised to use a VPN or RAS connection to enter the network, and then access your firewall from either your client session or a jump host. Of course you'll also want to restrict access on the internal trusted network to your systems using a trust side policy permitting access to the appliance only from trusted hosts. This negates the vulnerability.

## Behavioral discrepancy information leak

The Behavioral Discrepancy Information Leak documented on CVE impacts the appliance when using IKE with pre-shared key authentication. It allows an attacker to enumerate valid usernames using an IKE Aggressive Mode packet. This generates a response if the username is valid but does not respond when the username is invalid helping an attacker identify valid user names to attempt to exploit.

## FIX

The solution is simple. The vulnerability only impacts version 5.2 and below so again getting a unit with a valid build negates the issue. Of course this doesn't give an attacker access to the device or the VPN, it merely gives them valid user names to attempt to exploit but to fully mitigate the issue simply get a model running 5.4 or upgrade yours.

## Unknown Vulnerability in ScreenOS (CVE-2004-1446)

This is the one that many reference with the older Netscreens as it is in the dreaded "unknown" category. It is a DoS attack in that it allows remote attackers to cause a reboot or hang using a crafted SSH v1 packet.

## FIX

Usually you probably don't want to permit SSH direct to your Netscreen from the untrust zone. Even though it's encrypted it is preferable to have a different method of accessing the internal network then use either a jump host or a VPN NAT'd address to ssh into the appliance. Of course this is not always possible and it can often be necessary to SSH into the appliance and that's fine as again the issue is limited to version 5.0 and below (<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-1446>) so quick fix is to upgrade to ScreenOS 5.4.

There are other documented vulnerabilities on ScreenOS 5 but most are either at 5.0 or below and therefore are not an issue unless you don't have access to an upgrade. Of course the easy fix is to pick up a unit with 5.4 installed. Preferably you'll want 5.4r10, however any 5.4 version is fine since the few documented vulnerabilities are easily mitigated or negated.

This concludes part 1 of our brief look at the Netscreen and ScreenOS and "some" of its features (there are many) and how it compares to the Cisco PIX and PIX IOS. In part two we'll take a look at hardening the Netscreen, attack signatures (including a couple of really cool built in signatures) and defense protections and capabilities, some basic deployment scenarios where these application layer protections can be useful and finally some basic steps to get your Netscreen up and running in a basic web application services deployment and of course how the configuration examples compare with similar configurations both in implementation and syntax, with the PIX IOS.

---

## CHRIS WEBER

*Chris Weber is a freelance Network Security Consultant with more than 15 years in the field of network security, analysis and design and has consulted on network security issues and incident response for multiple commercial organizations including fortune 500 and fortune 100 firms as well as US Federal Government organizations. Mr. Weber has held multiple industry certifications throughout his career including Cisco, Microsoft and others, and is currently an authorized Juniper Consulting Partner. Currently Mr. Weber consults via his own freelance consulting firm "Layer 9" located in Northern Virginia and can be reached at [cw@layer9security.com](mailto:cw@layer9security.com).*



# Lint Center

for National Security Studies, Inc.™

EMPOWER, ENHANCE, ENABLE

## Need a scholarship?

*White hats, Ninjas, Grinders, and Engineers – listen up!*

The Lint Center for National Security Studies awards merit-based scholarships semi-annually in both July and January. A streamlined, web-based application form is available on our main portal. Undergraduate and post-graduate students pursuing technical degrees in computer security, computer science, diplomacy, and linguistics are encouraged.

**[LintCenter.org](http://LintCenter.org)**

**About the Lint Center:** The Lint Center for National Security Studies in the United States is a Veteran and Minority directed, all-volunteer 501(c)(3) non-profit organization, dedicated to fostering the educational development of the next generation of the National Security and Intelligence communities by providing passionate individuals with scholarship opportunities and mentorship from experienced National Security personnel.

### **About the Lint Center's Mentoring Program:**

In addition to the scholarship award, winners will acquire an experienced security practitioner-mentor. With over 150 mentors, the Lint Center is well positioned to match emerging leaders with practitioners to streamline the learning curve.

Check out our blog: [LintCenter.info](http://LintCenter.info)

Follow us on Twitter: [@LintCenter](https://twitter.com/LintCenter)

Become a fan: [facebook.com/LintCenter](https://facebook.com/LintCenter)

**EMPOWER, ENHANCE, ENABLE...**

*(Script Kiddies need not apply)*

# Reading Between the Lines

## How to quickly obtain what you are looking for when reverse engineering assembly code

Much like pondering time travel and staring into the Matrix, reverse engineering assembly code can be an overwhelming task. Many novice reversers get lost in the ocean of instructions and can take weeks to identify a simple print statement. However, there are shortcuts one could take to make the process less daunting and more efficient. By employing these methods, even the freshest RE stands a chance of defeating the monsters within the code.

### What you will learn...

- How to make sure you are looking at real code and not garbage
- How to view the code in a way that is pleasing to the brain
- How to rename subroutines so they are easy to spot
- How to leave breadcrumbs in the code by making comments
- How to work backwards by 'finding the cheese first'
- How to make your map complete by forcing the code to work for you

### What you should know...

- Have a firm understanding of operating system fundamentals
- Have a working knowledge of high level programming (C/C++)
- Be familiar with x86 Assembly
- Be familiar with the concepts, methods and tools of reverse engineering

An aspiring reverse engineer goes through an immense learning regiment, which includes learning about the inner workings of an operating system, mastering an arsenal of new and complicated tools and learning an array of different programming languages, the most important of which being assembly code.

Assembly is inherently easy to learn, there are only a few instructions that make up the dialed down version of a higher level programming language. However, even after arming themselves with all the tools required to reverse engineer a program, they are bombarded with their first look at disassembled code, a waterfall of PUSH's and POP's, MOV's and RETN's, the garbled, uncommented and (most of the time) not-completely intact nightmare that is RE.

### The solution

If you work in a setting where you are allowed to take 3 months to tear apart a program, good for you,

enjoy dreaming about the code! For everyone else who usually works on a deadline or does not have the time to examine every line of code, there is a better way. Just like when trying to write a report on a 500-page book in an hour, an RE needs to use a few parsing tricks in order to understand the flow and function of the program. These tricks seem simple enough in their execution but it is only with practice that they will become second nature and therefore most effective. The goal is to take shortcuts to find out parts of what you want to know, to understand the flow of the code and predict what the program might be doing next, which will allow you to skip the boring redundant instructions put in by the compiler and get straight to the good stuff.

### Tools

In this article, I will be talking about two tools in particular, they are my favorite and I always use them whenever I need to do some RE:

- OllyDBG – My Favorite Debugger
- IDA Pro – My Favorite Disassembler

In addition, here are some tools that I will be mentioning in this Article:

- PEID – Awesome binary packer identifier
- QUnpack – Awesome unpacking application
- GUNPacker – Another awesome unpacking application
- MSDN Library – The Microsoft Developers Network Library, you can install a local version that comes with Visual Studio or you can just search on the Web and find the web version, either way it is incredibly useful and you should definitely have access to it.

## Note

This article will also only focus on reverse engineering Intel x86 Assembly, it is the most common type of assembly you are likely to run into when reversing anything written in C/C++.

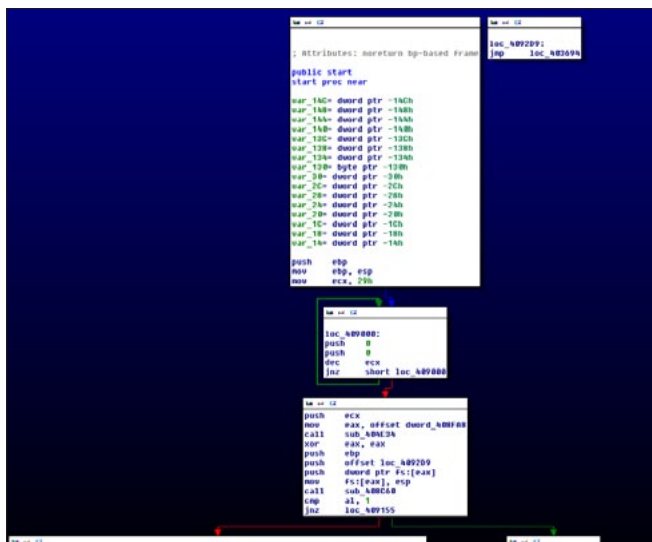


Figure 1. IDA Pro Function Graph View

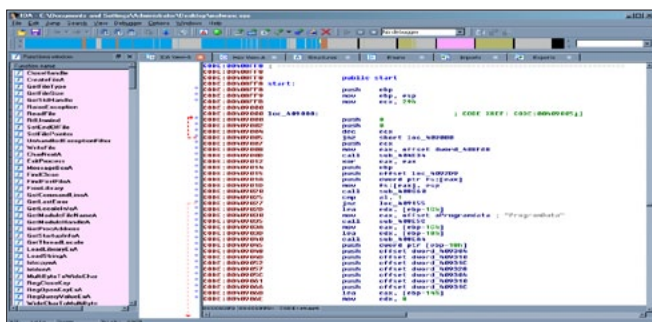


Figure 2. An example of IDA Pro not recognizing a function



Figure 3. The end of a function without a RETN

## Pre-Game Stretches

Before you attempt doing any kind of reversing, you need to make sure you are going to be looking at real code, not garbage. To do this, I usually do a few things:

- Throw the binary into PEID, it will tell you if the binary is packed.
  - If the binary IS packed, unpack it when one of the unpack applications listed in the Tools section.
- If PEID says everything is okay, try opening the binary in OllyDbg, you need to make sure that the file is valid.
  - If OllyDbg cannot open the file, it might be corrupt or just not executable.
- Finally, open the file in IDA Pro and check to see if everything is loaded properly, you should see at least one export function, maybe some imports and sections of real code.
  - If everything in IDA Pro is garbled or all you have is a tiny function and no imports, you might have a custom packed binary.
  - If you have a custom-packed binary, there is one thing to remember: *every packed binary must be unpacked before it can run.* Therefore, a good way to unpack something unique would be to let it unpack itself.

To sum up, the only time you should be attempting to reverse engineer a packed binary in IDA Pro is if you are trying to figure out how to unpack it; NEVER try to parse through packed code, it will get you nowhere and you will waste a lot of time.

## Creating order from chaos

One of the greatest things about IDA Pro is its ability to automatically create a flow-chart type graph to view the assembly code (Figure 1). It takes a function and puts it into a box with all the assembly inside of it, and then when it encounters a conditional jump, IDA will create new boxes for the results of that jump, one for true and one for false. The purpose of this functionality is so that humans can easily determine the flow of a function instead of having to manually do it ourselves and waste brain power by keeping a mental note of whether the “Jump if Equal” statement is true and do we need to jump to the code at 0x00401123.



While that is just one of the many amazing things IDA Pro can do, it does not make IDA as smart as a human. You have to keep in mind that it does not always recognize a function when it sees one. You might load up a binary and find the 'Start' function is in line-by-line assembly mode rather than the graph. Figure 2 shows you exactly what this looks like. You can hit the space bar a hundred times and IDA will refuse to make it look nice for you. In this case, you need to know how to make IDA realize that a function is there.

IDA has a command called "Create Function" which it allows you to execute if you select a portion of code from the start of it to the end. All you need to do is highlight the code using your cursor. After that, scroll down with your trackball (if you have one) to where you find either no-code or another function starting, we hope that there is a `RETN` instruction to neatly signal the end of the function but sometimes there isn't and you just have to deal

with that. Figure 3 shows an example of that disappointing situation.

When you find the end of the function, right click on the selected area and select "Create Function." The resulting graph will represent the function you just selected. This allows you to worry less about the flow of the application and more about the purpose of the function (Figure 4).

## Keeping Track

If we are going to be hopping around the code constantly looking for new and interesting functionality, we need to be able to keep track of where we are for our own notes as well as being able to navigate the same straits later on when using OllyDbg. Unfortunately, when we switch to graph mode, we lose the ability to see the address of the code we are looking at. Beyond hitting the space bar every time we need to check our location, we can just modify some of IDA Pro's general options. In order to do this, make sure you are in graph mode and click on the "Options" menu then click "General" (Figure 5).

This opens the IDA options interface where you can select the "Line Prefix" option (Figure 6); this will show us the location of each line of code on the graph display. Another nifty option you could select is "Auto Comments" which gives very general and

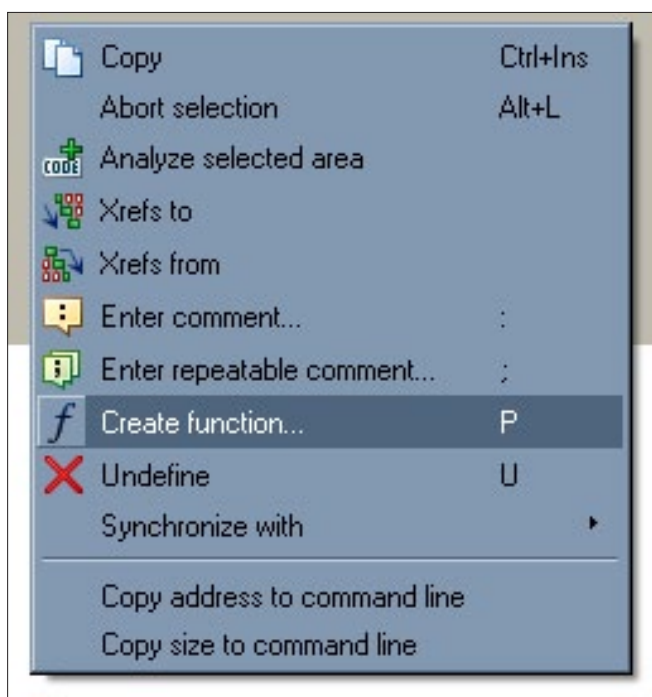


Figure 4. 'Create Function' Option

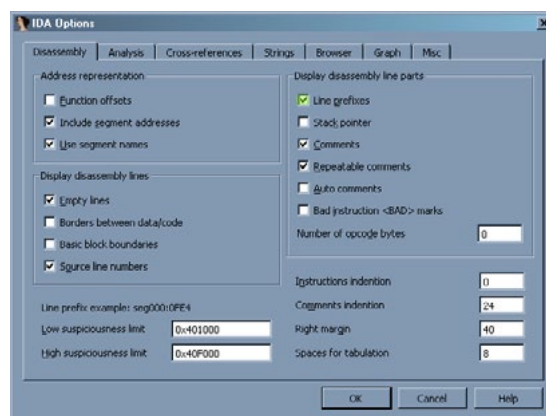


Figure 6. IDA Options interface

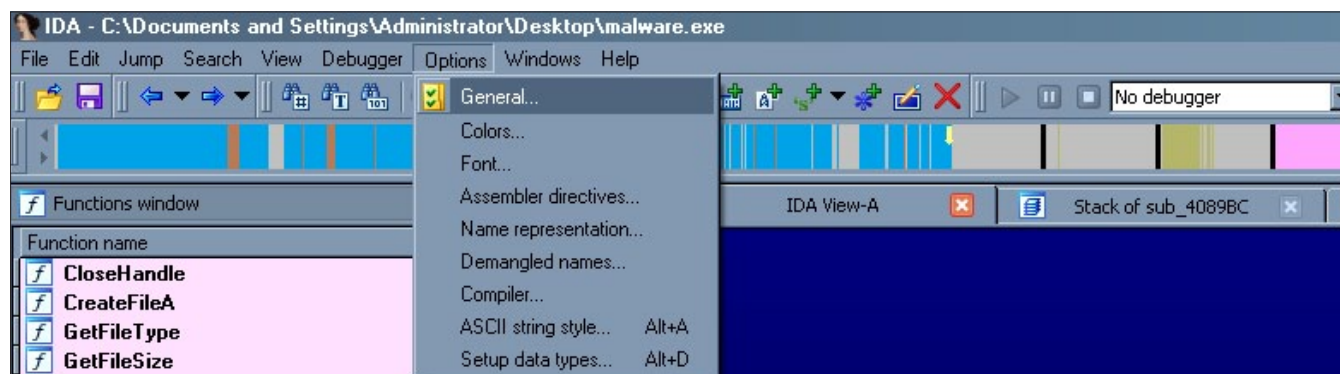


Figure 5. The Options->General Menu Item

technical comments on certain lines of code; this would be useful to someone who is not as familiar with assembly.

Keeping track of the location of the code is incredibly useful when trying to get a deeper look into the code by using a separate application such as a debugger or just keeping track of interesting functions that you might want to examine further later on.

## Give me the Gist

Imagine walking through a small city you have never been to before and all of the buildings have no descriptions other than “Building <number> E. Street”, how would you know what function they served and how could you tell if they were important or not? To make it even more frustrating, imagine that some of the buildings are duplicated at different intervals throughout the city so you would not know if you had even been to that building before or not.

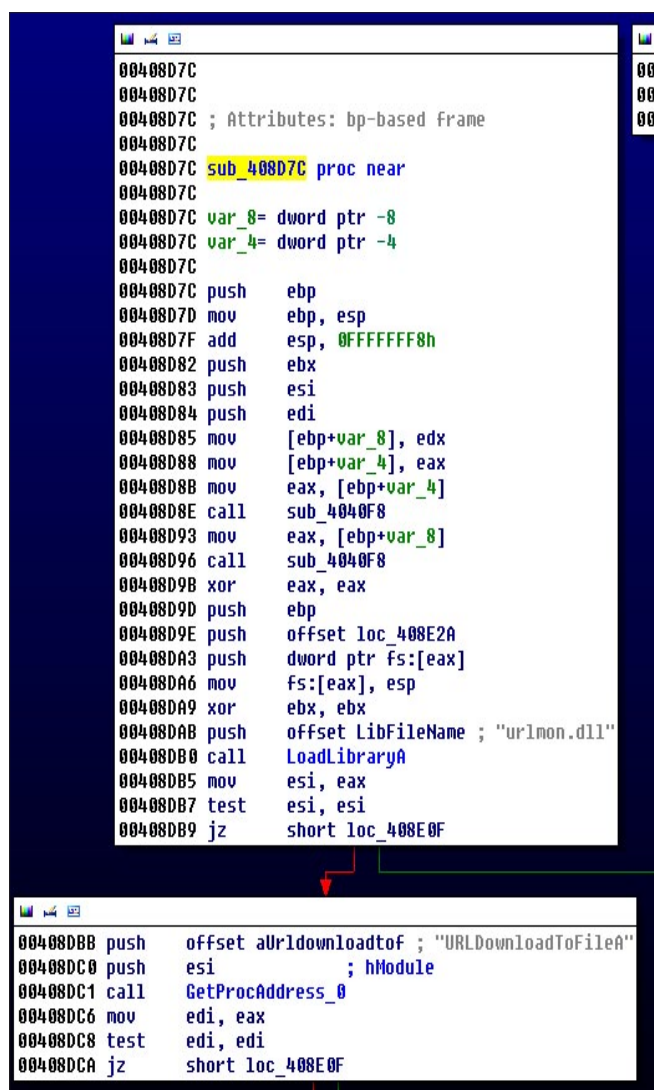


Figure 7. A function with a default name

Well this is not that different from reversing a new binary. Each function that is part of the original programming and not a Windows API usually starts with the prefix “Sub” (for subroutine) and then the address where the function is located in memory.

The best way to avoid overlooking functions with non-descriptive labels is to rename them something that means something to you. In Figure 7 you can see an example of what IDA Pro will automatically name a function, if the function is repeated numerous times you may begin to remember the address but what if it’s a unique function, only used once or twice in the program? Well we can rename the function by simply right clicking the function name and selecting the “Rename” option or pressing the “N” shortcut key (Figure 8).

Now that you can rename the function, what should you rename it to? I generally try to use the purpose of the function, as you would if you were programming a new function. If you notice on Figure 7, one of the functions of this routine is to resolve the API `URLDownloadToFile` and later on it actually makes that API call. Based on that information, I called this function `DownloadFileFromURL` because that is what it does. The name is up to you, I enjoy using this method but in case of running into a function that I cannot identify, I will often use the name `IDontKnow`.

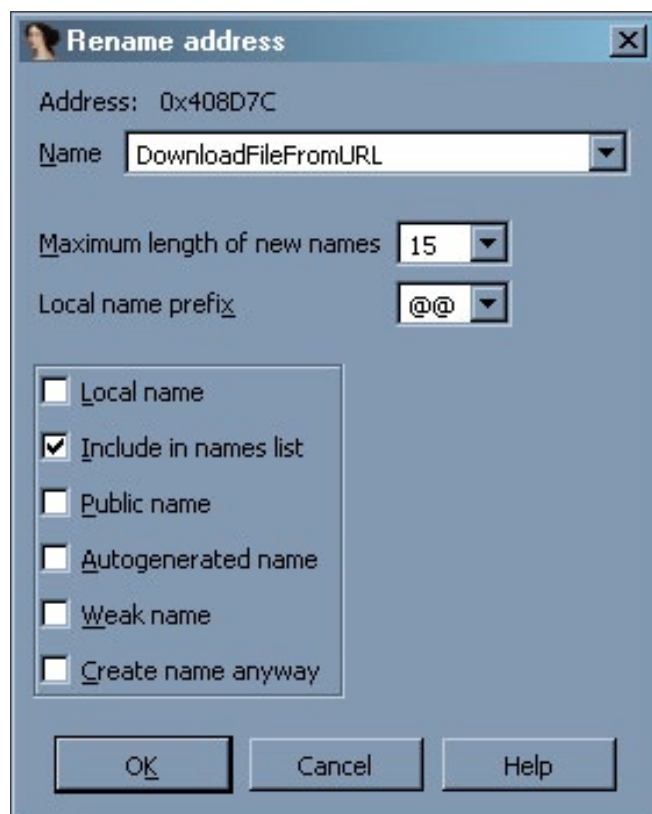


Figure 8. The rename address interface

Another benefit of renaming the functions is being able to identify them in other functions, which can help you rename those to something more important and help you understand the flow of the program even better (Figure 9).

## Commentary

Commenting is a programmer's best friend or worst enemy. Some programmers hate to do it and others do it a little too much, either way it is an important part to understanding the code and how it all works together. When it comes to reverse engineering, the same principals apply; commenting will always benefit you. You can comment anything, be it what values are being passed, the purpose of a certain group of API calls or arithmetic operations or even just your own theories on the where the code is leading. Personal notes are useful in case you lose your train of thought or if you step away from the code for a while. If you really enjoy commenting, you could even write comments insulting the code for being so weak against your Jedi reversing skills!

IDA Pro makes comments easy, it does not matter if you are using the graph interface or going through the code line-by-line.

In Figure 10, a function that I named "CheckOSVersion" is checking for a specific value after calling the API `GetVersionExA`. I found out what the compared value (0x06) referred to by looking up the API call in the MSDN library. I discovered that the value refers to any Windows operating system released *after* Windows XP (Vista/Win 7/etc). If I were to stop reversing at this function and go on a vacation or even just look away momentarily, I might forget what that value means. If so, it is important that I make a note to myself in the com-

```
CODE:00409078      mov     edx, [ebp+var_14]
CODE:0040907B      mov     eax, offset aHttpDl
CODE:00409080      call    DownloadFileFromURL
CODE:00409085      lea     edx, [ebp+var_28]
CODE:00409088      mov     eax, offset aProgramdata ;
CODE:0040908D      call    sub_408E5C
```

**Figure 9.** The renamed function shown inside of another function

```
00408C60
00408C60
00408C60
00408C60 CheckOSVersion proc near
00408C60
00408C60 var_94= dword ptr -94h
00408C60 var_98= dword ptr -98h
00408C60
00408C60 add     esp, 0FFFFFF6Ch
00408C66 mov     [esp+94h+var_94], 94h
00408C66 push    esp ; lpVersionInformation
00408C6E call    GetVersionExA
```

**Figure 10.** CheckOSVersion calls an API to determine the OS Version

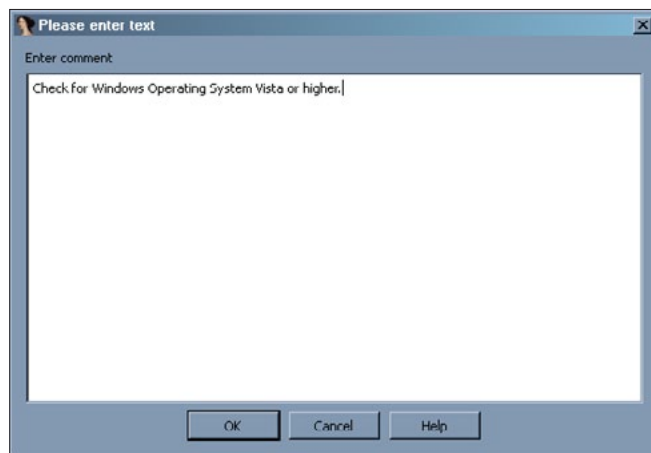
ments that the code is checking for a certain type of operating system.

To make a comment, right-click the line of code you want to make a note on (to the right of it in the whitespace) and select the "Enter Comment" option. When you do that, a text box appears where you can write in your comment. Figure 11 shows what I wrote and Figure 12 is the result. After adding the comment, I even felt inclined to change the name of the function to reflect its purpose.

Commenting is not just something that school kids and people with bad memories should use. It is very easy to get lost in the code and if you have not already left yourself a note of why a particular function is important or what it could do, you might end up looking up the same values repeatedly. Do your best to be efficient and not duplicate your work if you do not have to.

## Finding the Cheese First

Okay, after renaming your functions, commenting the code heavily and making sure that every piece of code is in an easy to look at graph format, you still have no idea what is going on with this program. This happens a lot and even with the previously mentioned techniques, you could spend hours wandering aimlessly in the code. In these situations, it is best to think about your exact title, Reverse Engineer, literally meaning to engineer something in reverse. So if you are sup-



**Figure 11.** Comment entry interface

```
00408C60
00408C60
00408C60
00408C60 CheckForVistaOrHigher proc near
00408C60
00408C60 var_94= dword ptr -94h
00408C60 var_98= dword ptr -98h
00408C60
00408C60 add     esp, 0FFFFFF6Ch
00408C66 mov     [esp+94h+var_94], 94h
00408C66 push    esp ; lpVersionInformation
00408C6E call    GetVersionExA
00408C73 cmp     [esp+94h+var_90], 6 ; Check for Windows Operating System Vista or higher.
00408C78 setnb  al
00408C7B add     esp, 94h
00408C81 retn
00408C81 CheckForVistaOrHigher endp
00408C81
```

**Figure 12.** The result of my commenting



posed to be doing this all backwards, why are you moving through the code in one direction? This is where the trick of finding your end goal and working backwards comes into play. In my opinion, this trick is the best way to figure out ex-

actly what is going on with a binary in the shortest amount of time.

Imagine that you were a mouse trying to find your way through a maze to find a piece of cheese, the cheese in this metaphor of course being the execution of a particular function. You make your way somewhat into the maze but find that you do not know where you are going, so instead you start at the other end, where the cheese is, and work your way backwards to a familiar part of the maze. On the way, you leave pieces of the cheese as markers to illuminate the correct path. At this point, you would know how to navigate through the maze successfully and could easily do it again if you needed to.

The same method in which the mouse found the cheese and worked backwards can be employed in reversing. In order to accomplish this, use the "Imports" tab in IDA Pro. The imports are all of the API functions that the binary needs to use in order to do complete its operations; Figure 13 shows you what this tab looks like.

IDA Pro not only knows about these functions but also knows where they are being called in the code; you can use this to your advantage. By double clicking a function related to what you want to

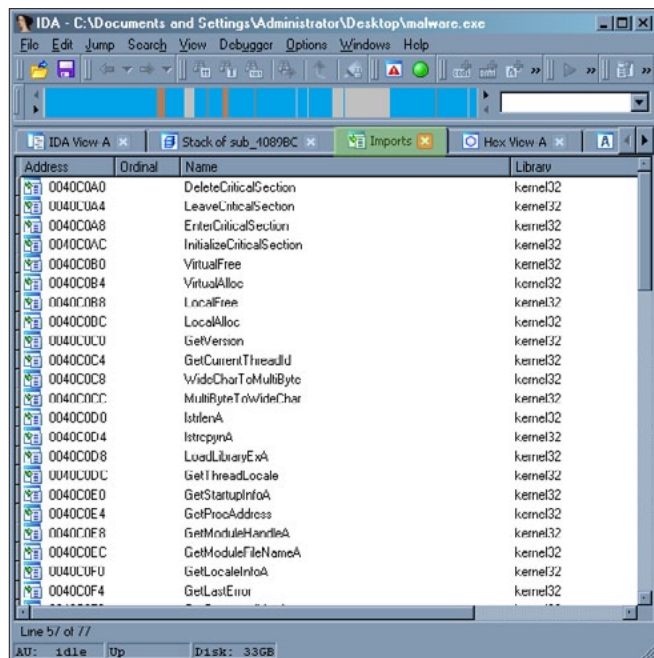


Figure 13. The IDA Pro Imports tab

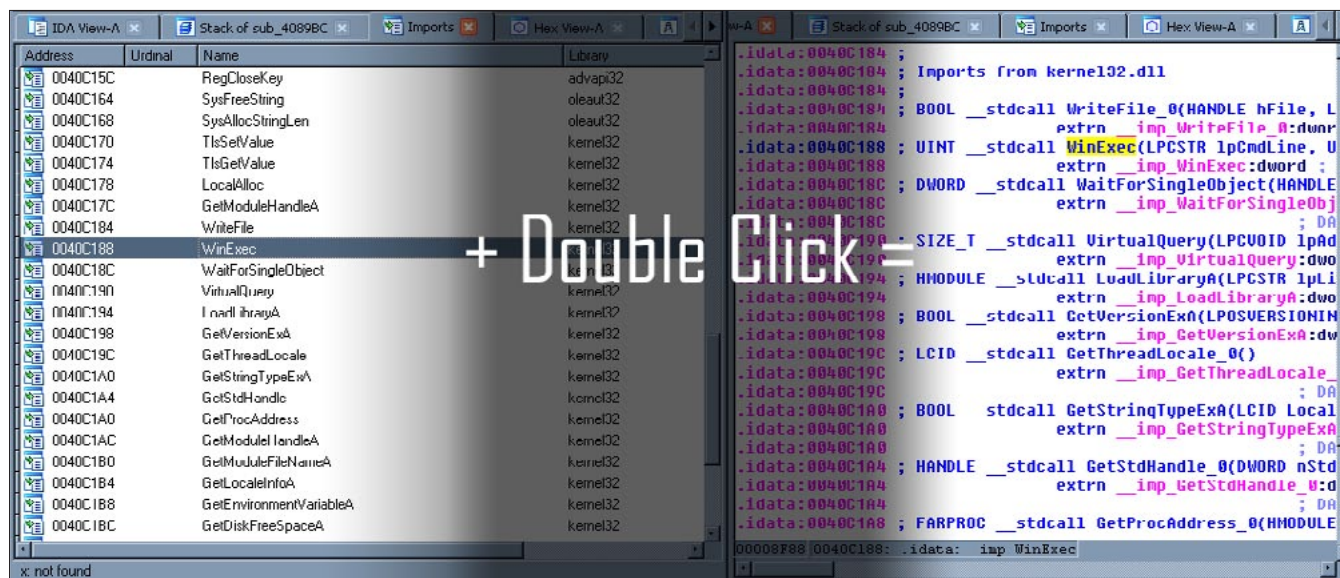


Figure 14. How to find the API function declarations

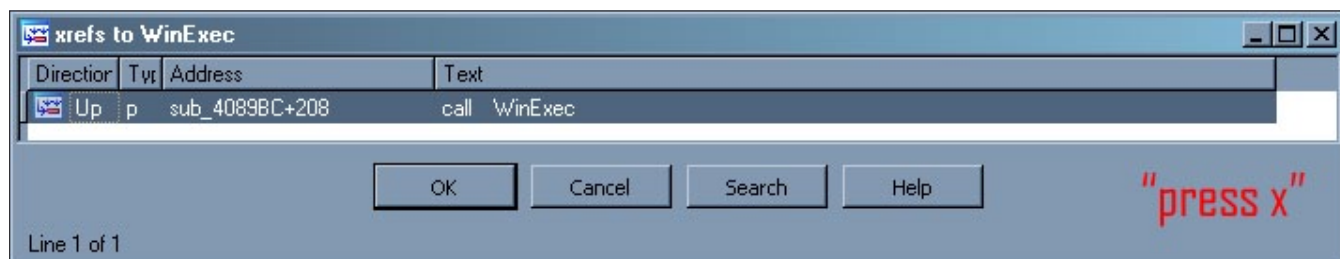
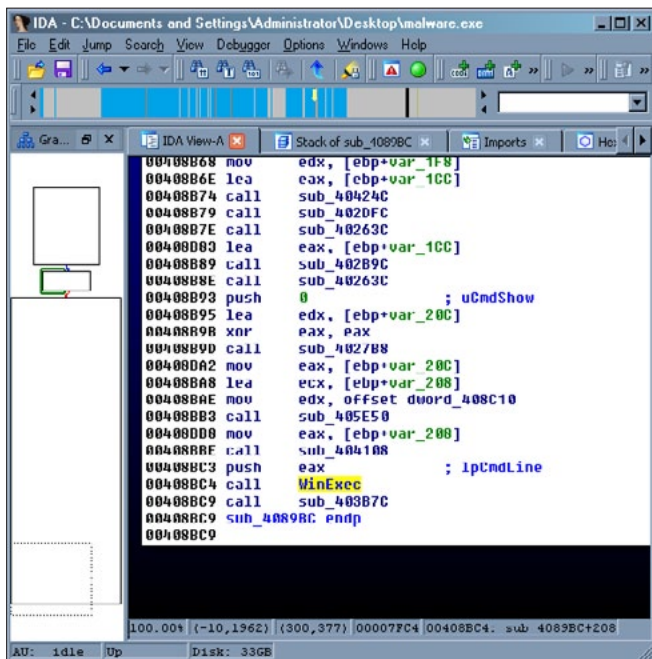


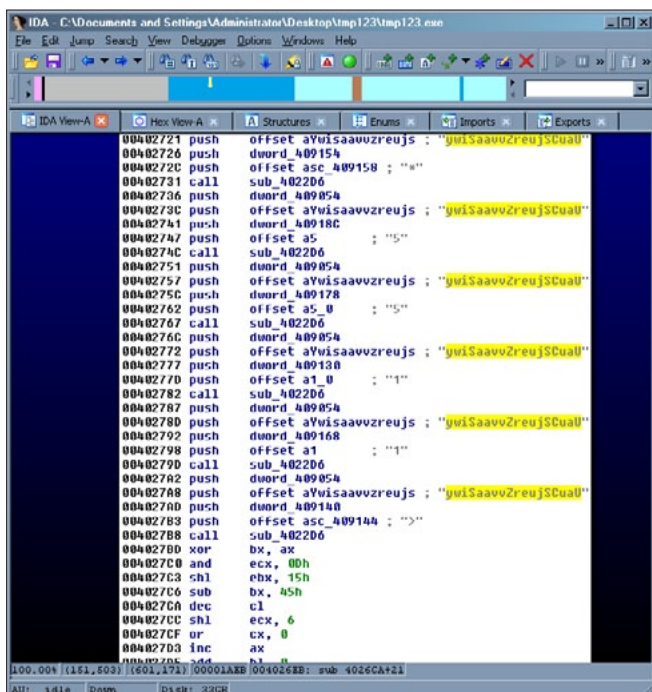
Figure 15. The IDA Cross-Reference results for WinExec

find out about, it will take you to a very pink group of API functions declarations. From there you can use IDA to cross-reference the API functions with the calling code.

In Figure 14, I want to know where the API function `WinExec` is being called. I double clicked the function name and was taken to where the function was being declared. In Figure 15, I have pressed the “x” key and IDA told me all the places where `WinExec` is being referenced. In this case, there is only one function using it.



**Figure 16.** *The portion of code that calls WinExec*



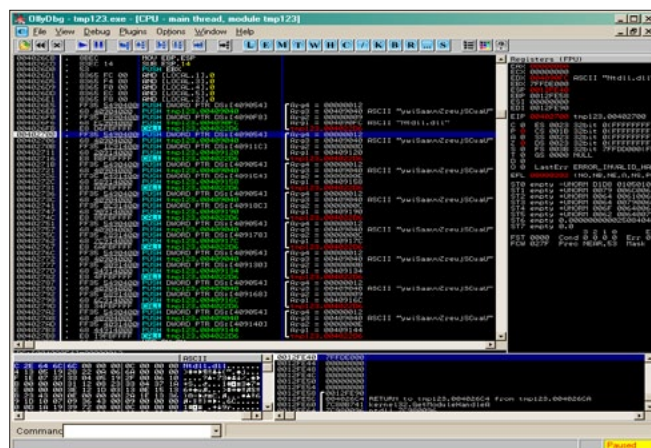
**Figure 17.** The function that calls a decryption routine to resolve dynamic API function names

Next, I double clicked that result and was taken to the actual function, where I saw exactly how `WinExec` was being used and what other types of functions were being used in conjunction. My next step was to comment and rename the function, then use the “x” key again to find any cross-references in other functions, renaming and commenting until I work back far enough to somewhere I have been before or can easily get to. This method does not just work with API calls either, if you look in the “Strings” tab, you will find a list of different strings that IDA has extracted from the binary and it will tell you where those are being referenced as well (Figure 16).

## Filling in the Blanks

There are certain types of programs, namely malware, which will do everything in its power to make it more difficult for you to “find the cheese.” There are numerous reasons for this, maybe the author does not want someone else stealing their code or maybe they do not want someone to find out the true capability of their program, either way it creates a big problem for reverse engineers. These anti-reversing techniques usually take the form of dynamically created addresses, function calls and even mathematical operations. If you encounter something like this, you might not be able to continue using only IDA Pro. In these cases, I recommend using a debugger like OllyDbg. In Figure 17, the program uses a decryption routine using a hard-coded key value and a single character value to represent an API call.

At this point, I would open the binary in OllyDbg or another debugger and using what I already know about the flow of the program, navigate to that portion of code and let the binary decrypt the values for me. Figure 18 reveals what the API function names are and from there I can comment the



**Figure 18.** OllyDbg executing the code and resolving the dynamic values for me



code in IDA or rename the variables where the results are stored so I know which one is being referenced, no matter where I am in the code.

Keep in mind that IDA Pro also has a very powerful debugger and many Reverse Engineers swear by it, however I recommend keeping your debugger and disassembler separate only because when dealing with certain types of programs (malware) you might damage or corrupt your IDA file and lose all your work. I keep them in two separate virtual machines, frequently save, and backup the saved IDA file to a remote drive.

## Conclusion

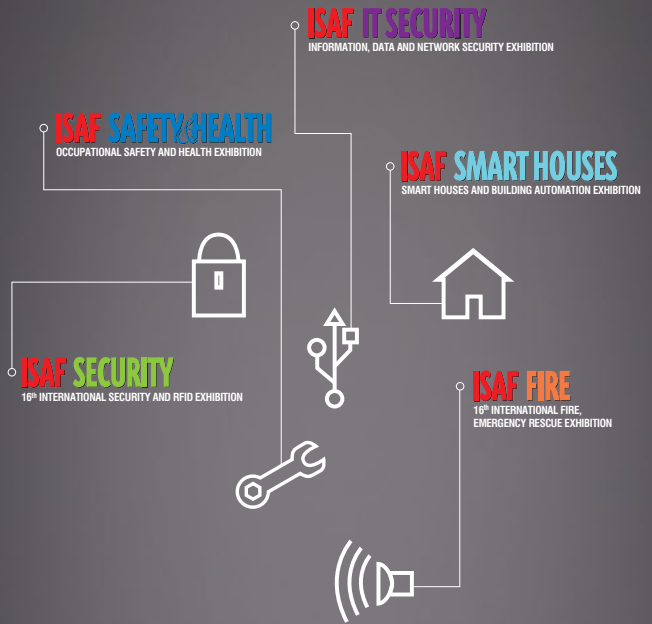
So there you have it, an array of different tips and tricks that you can use to help you get what you want out of assembly code. As far as what you should do next, that is up to you. The method in which an RE completely tears apart a binary is always their own. Each person is different and the way we perceive and come to conclusions are different. Being an RE is like being a detective, putting the pieces of a puzzle together in order to see the bigger picture. I know many Reverse Engineers who prefer to take a completely static approach and only use IDA Pro. I also know plenty who prefer to use IDA Pro as a map, making as much sense of it as possible beforehand and then using it to guide them through the code using a debugger, editing and adding to the map as they go. In the end, it is whatever works best for you; remember that RE is an art form as much as it is a technical skill and it takes practice, passion and continuous education to become good at it.

## ADAM KUJAWA

*Adam Kujawa is a computer scientist with over eight years' experience in reverse engineering and malware analysis. He has worked at a number of United States federal and defense agencies, helping these organizations reverse engineer malware and develop defense and mitigation techniques. Adam has also previously taught malware analysis and reverse engineering to personnel in both the government and private sectors. He is currently the Malware Intelligence Lead for the Malwarebytes Corporation. [akujawa@malwarebytes.org](mailto:akujawa@malwarebytes.org).*



The **Most Comprehensive** Exhibition  
of the Fastest Growing Sectors of recent years  
in the **Center of Eurasia**



[www.isaffuari.com](http://www.isaffuari.com)

**SEPTEMBER 20<sup>th</sup> - 23<sup>rd</sup>, 2012**  
**IFM ISTANBUL EXPO CENTER (IDTM)**



T. +90 212 503 32 32 | [marmara@marmarafuar.com.tr](mailto:marmara@marmarafuar.com.tr)  
[www.marmarafuar.com.tr](http://www.marmarafuar.com.tr)

THIS EXHIBITION IS ORGANIZED WITH THE PERMISSIONS OF T.O.B.B.  
IN ACCORDANCE WITH THE LAW NUMBER 5174.



# How to Protect Your Identity in the UK from Fraud

Information is being collected about us every second of every day without us ever realizing what happens to it. Most of us don't really care what happens to our personal data as long as it isn't misused. So let's go up close and personal by taking a brief glance at how you can protect your personal data if you are a UK citizen.

**W**orth remembering, your data held in the UK is also shared with other countries, mainly the English speaking world i.e. Canada, New Zealand, USA, South Africa and Australia to name a few. The credit reporting agencies share this data with these countries and in particular when people migrate to these countries. Every country has its own data protection laws but for the benefit of this article we will concentrate on the UK.

## UK data regulation

Regulating our personal data is more important than ever these days, especially given the sensitive nature of the data that is collected. The first attempt at a data protection law was with the *Data Protection Act* (DPA) 1984 which started by authorising organisations to take accountability for your personal data privacy. Check any UK registered website and they should highlight the DPA 1984 and 1998 (amendment). The 1998 amendment tightened the DPA which now allows everyone to see the data that is stored about them on either hardcopy (paper) or a computer.

The personal data held by third parties is used in many instances to make key life changing decisions without you ever realizing it – i.e. credit referencing agencies, people tracking websites, banks, mortgage lenders, employers etc. I will discuss this in more detail later. The DPA provides a safeguard for people so people can ask for the data held about

them and dispute any inaccuracies. The way the data is collected and used is also covered under the DPA 1984/1998 Acts. As is the case with most laws, it's there as a protection but that doesn't stop data breaches or inaccurate data being held about people.

## Keep in mind

You can use the DPA to request information from a financial provider if you suspect for example that the data about you is inaccurate. It doesn't have to be your data that stops you from being accepted for a new loan or credit card. It can also be where you live and who you live with. More often than not people fail to tick or un-tick the 'do not receive any marketing communication from a company or its third parties' box. You should always remember to 'opt-out' if you value your privacy.

## The Electoral Register

There are many instances of people applying for credit cards and loans being refused simply because they are not recorded on the electoral roll. The electoral register should highlight your current address, so it's important you make sure it's up to date if you have recently moved. The names and addresses of all UK citizens over the age of 18 registered to vote are kept on the electoral register <http://bit.ly/qcw51>. For the past few years organisations and individuals could obtain this in-

formation and use it for any legal purpose, but privacy concerns have meant that regulation was introduced in 2002.

The regulation introduced two electoral registers. The full register lists everyone who is entitled to vote. Only certain people and organisations (i.e. UK Direct Marketing Association <http://bit.ly/BM-RXz>) can have copies of the full register, and they can only use it for specified purposes. These include electoral purposes, the prevention and detection of crime and checking your identity when you have applied for credit. The edited register leaves out the names and addresses of people who have asked for them to be excluded from that version of the register. The edited register can be bought by anyone who asks for a copy and they may use it for any purpose.

Everyone on the full register goes on the edited version by default, but you can 'opt out' this when you return the 'Annual Voter' registration form. This means commercial organisations will not be able to have access to your name and address and on that year's register. Remember, that you will not be removed from the previous year's registers. Organisations may still have your personal details as well as the people you live with. If you want to stop cold calling, direct marketing mail and tempting credit card offers, this is a first positive step to protecting your personal data.

### Preference Services

Register with the free MPS (Mailing Preference Service) <http://bit.ly/3xksTZ> if you want to manage and control what marketing mail marketing telephone calls (includes silent calling) you receive. This list of people who don't want their publicly available details to be used for direct marketing purposes is administrated by the *UK Advertising Standards Authority* (ASA). There is though one small issue with this and that is organisations are not legally obliged to use it.

UK organisations can buy in the lists but should check the data against the Mailing Preference Service opt-out list. The problem is a number of organisations don't actually do this. That said if the organisation is a DMA member (and you can check to see if an organisation is a member of the DMA <http://bit.ly/7tzoa0>) they are bound by the code of practice, so must screen the data against the MPS database.

The Royal Mail also has an 'opt-out' door to door service <http://bit.ly/UU3g6> which will stop all those unaddressed mail being posted through your mailbox. This service doesn't stop the mail addressed 'the occupier' though. If an organisation continues

to send you unsolicited marketing mail after you asked them to stop, that organisation will be in contravention of the Data Protection Act and ASA regulations, which means that the ICO and ASA can be asked to intervene.

Another really useful mailing preference service is 'The Bereavement Register' <http://bit.ly/hmlbcW> which can help reduce the amount of direct mail sent to your address, stopping painful daily reminders. Unless companies are informed of a death, they will continue to send promotional mailings about their products and services. By registering with this free service the names and addresses of the deceased are removed from mailing lists, stopping most direct mail within as little as six weeks.

### Telephone marketing, silent calls and filling in forms

Telephone marketing calls are something we all have experienced. Sometimes having an ex-directory number can help as can signing up for the *Telephone Preference Service* (TPS) <http://bit.ly/qOsfT> Organisations are not obliged to use the TPS list but it does help reduce the marketing calls from personal experience. If you are repeatedly hassled by these marketing and silent calls then complain to the ICO.

Cold calling that originate overseas can also be stopped, but only if those companies calling are UK registered/owned and are using foreign call centres to make these calls – so these companies will still be bound by the DPA code of practice. If you are still receiving cold calls then there is an EU Data Protection Directive <http://bit.ly/QqxGe> which the ICO routinely liaises with.

Silent calls are made by automated dialling systems that fail to connect the call when answered, however it might a good idea to register with a service called SilentCall-Gard: <http://bit.ly/eH5aG> – it's totally 100% free. In the UK, new legislation introduced by the regulatory body Ofcom (Independent regulator and competition authority for the UK communications industries) has just revamped the automated dialling systems. After February 2011, all automated calls must be connected within two seconds of the recipient speaking or there should be a recorded message that states the organisation's name and how to opt out of future calls.

Form filling is something we are all fond of – well not really. This is where we get caught out as so far as allowing others access to our personal data by forgetting to tick or un-tick a simple box. Be sure to tick the appropriate boxes when filling out

any forms for goods and services. Look for opt-out statements which use euphemisms to confuse you. Read the opt-out a couple of times so you fully understand what you are opting out of and that you are actually not opting in. It's very important you have the opportunity to prevent your details being passed to third parties – but this is in your control. Consider this; magazine subscriber lists are routinely sold / rented as are our high level data from our credit files to marketing and other agencies (including people tracking websites). Form filling will never go away, whether it's online or a paper copy, so stay completely vigilant.

### HINT

Worth noting and not everyone knows this – third-party organisations are not legally allowed to sell on the details of consumers on these sold-on lists, unless that is they convert these consumers into consumers of their own.

### Checking your credit report

Under the DPA you can request information from a financial provider i.e. bank, credit card provider if you suspect the information about you is incorrect or has caused you problems when applying for a loan, credit card or opening a bank account for example. The Data Protection Act allows for you to obtain a 'statutory credit report' from all the credit reporting agencies – Experian: <http://bit.ly/hN-L28g>, Equifax: <http://bit.ly/fY7yZq> and CallCredit: <http://bit.ly/gRlv2c>. The information on credit reports is the most important information about you. Credit information is used to decide whether you are financially viable. In other words these agencies decide whether you can have a loan, mortgage, credit card and so on. Without a credit history (which takes time to build – and the only way to build this is to have credit in your name) you are unlikely to be able to borrow money.

Credit card companies are not that interested in people who don't rack up debt – so long as they can make money on your interest payments they are more than happy to give you credit to spend. To access your statutory report will cost £2.00 (correct as of September 2012) but this will not give you your credit score – which determines how risky you are to loan money too. All three credit reporting agencies will have some different information about you, so it's important to obtain the reports and credit score from all three.

If you spot an error, you should send the credit reporting agency a 'correction' letter or if you notice that you have some late payments showing or you have an unpaid debt that was a result of an

uncorrected billing error. You can also apply to the agencies for a 'notice of correction' to your credit report which will clarify the in correction to future lenders.

If you have recently divorced or left your partner you should also 'financially disassociate'. Once a disassociation has been created, lenders requesting your report no longer see details of the disassociated family member or members. You will need to notify each agency about the disassociation.

If you don't do this then your ex-partner may obtain a loan or credit card in your good name. It has happened and continues too, even when people are legally divorced. Here are the links for financial disassociation: Experian – <http://bit.ly/dlakAB> Equifax: <http://bit.ly/eoU9Ds> CallCredit – <http://bit.ly/hDm03Z>.

### Protecting your email address

Unsolicited direct marketing mail is not only sent to a letter box. As we all know well it is also sent to our mail inbox on our PCs. This unsolicited email is called spam. Since 2003 sending spam is a criminal offence, but beware it all depends on whether you remembered to tick or un-tick that box on the web form that asks you for permission to use your personal details for marketing purposes.

Savvy surfers use two email addresses – one for email communication and the other with everything else. Disposable email addresses are a must have if you value your email addresses. There are many but the general idea is that you open a web page and click a get link for a randomly generated email address that exists for a specified time period. Here are three popular websites: Guerrillamail <http://bit.ly/2LVUNc> Spammogourmet: <http://bit.ly/PcE9K> and Mailinator: <http://bit.ly/1WHWBe>.

Some of these sites only allow you to send and receive email using their webmail system – but some not all allow you to manage the spam and forward any relevant emails to your actual email address.

### Facebook and Google data privacy

Facebook privacy has been the subject of much discussion in recent months. It isn't the only social website that is facing criticism. Google, the world leader in Web search, has been in trouble recently for collecting information from unsecured wireless networks all over the world. This was done as specially equipped vehicles took pictures for the Google mapping feature called Street View. Google said it never meant to collect people's private information, like e-mails and passwords.



Some of the main problems have been linked to the default privacy settings in Facebook. Facebook now opt out users in to allowing third party sites like Yelp to 'personalise' a user's experience, and there are questions about how much information is being given away. One suggestion here is to make instant personalization which exports users content to third-party Web sites, opt-in by default. Another data issue circulating is the one concerning third-party applications Facebook currently stores the data for no more than 30 days and does not use it for advertising or selling to third-parties. One suggestion here is for Facebook not to keep data about user visits to third-party sites that use social plug-ins, such as the "Like" button.

Facebook data privacy could also be enhanced if it was allowed to degrade or fade in time. The idea of "degrading" data about visitors isn't a new concept. A database could be developed that would gradually swap user details for more general information and help guard against accidental disclosure. See my blog entry regarding Facebook scraping <http://bit.ly/gWhq7W> for further information on this threat.

Facebook has recently addressed a major security issue – surrounding HTTPS. I wrote about this in *Managing your Facebook Privacy* back in June 2010 feature See my blog entry regarding how you can setup a HTTPS connection: <http://bit.ly/hVkkCB> – if we all value our data then we should all be using HTTPS.

### Protecting your identity and your personal data from identity theft

So – how do you go about protecting your good name, both in the cyber world and the offline world? I'm going to highlight the UK service options and then you can decide which service is best for you.

#### UK Identity Theft Protection Service Options

Here is what you should look for if you are living in the UK:

- Credit reporting / scores i.e. providing single report or triple reports analysis\*
- Computer protection i.e. anti-malware/firewall/anti-virus/password protection
- 24/7 access to trained ID Theft Resolution Specialists – includes identity recovery
- Identity theft Insurance (up to £50,000)
- Lost wallet/cards protection – will cancel and replace your cards/passport etc
- CIFAS Protective Registration – places a warning flag against your credit file(s)\*\* Also avail-

able for directors whose company is at risk of corporate identity fraud and against the name of any deceased party (by a relative or executor) who may be at risk of impersonation attempts.

\*If an application for credit is made in your good name you also have the option of receiving an EMAIL or SMS. The three leading credit reference agencies in the UK are: Experian, Equifax and CallCredit. \*\*CIFAS Protective Registration can also be purchased separately for £20 for one year. Please check the CIFAS <http://bit.ly/hHORFO> website for further information. (September, 2012).

The average cost of UK identity theft protection services varies from £8-10 per month (this mainly applies to credit monitoring only). In the UK there is only one company that offers an identity protection service, similar to what is on offer in the US – called Garlik. Garlik charge £4 per month for one year for individuals to DataPatrol. Garlik DataPatrol *DOES NOT* offers an online credit monitoring service. (September 2012).

#### Worth remembering

If you do decide to purchase just a credit monitoring service you will have to pay extra for your credit score.

#### Worth remembering

Section 75 of the Consumer Credit Act 1974 protects consumers on any credit card purchases (this includes loss or theft) which cost over £100 and under £30,000. Note: This also applies when someone else fraudulently uses your credit card i.e. Chip & Pin fraud, Card Not Present (CNP) fraud etc.

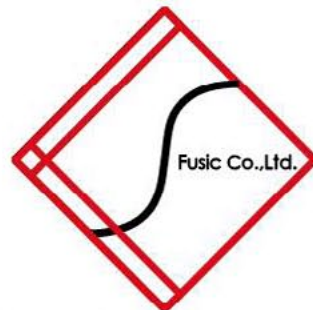
If you are a UK citizen and value your personal data, I'm sure what I have written here will be of considerable interest. I hope to cover this feature for US citizens very soon...

---

**JULIAN EVANS**  
*ID Theft Protect*

# Fusic

Fusion of Society, IT and Culture



Founded in 2003 in Fukuoka, Japan. Fusic provides several IT related services all around Japan. Among the services we provide are: web development, contract-based software development (such CMS and CRM), etc. We also developed our own web-based presentation service "Zenpre", and e-Commerce platform "Ureru-net-kokoku-tsukuru", and serve consumer through ASP. Currently, we also play a leading role in the mobile applications development in platforms such iPhone and Android.



浜崎 陽一郎

**Yoichiro Hamasaki**

Vice-President  
Co-Founder



内富 貞嘉

**Sadayoshi Noutomi**

President  
Founder

**Fusic Co.,Ltd** <http://fusic.co.jp/> [info@fusic.co.jp](mailto:info@fusic.co.jp)

**Fukuoka Head Office**

Shin-nihon build.9F, 2-4-22 Daimyo Chuo-ku, Fukuoka-shi,  
810-0041, JAPAN  
+81-92-737-2616 +81-92-737-2617

**Fukuoka Laboratory**

East Fukuoka General Office 4F, 1-17-1 Hakata Station East, Hakata-ku, Fukuoka-shi,  
812-0013, JAPAN

**Tokyo Branch**

Okura build. 3F, 1-4-10, Shibadaimon, Minato-ku, Tokyo, 105-0012, JAPAN  
+81-3-6450-1633 +81-3-6450-1634





# **HIGH-TECH BRIDGE<sup>®</sup>**

**INFORMATION SECURITY SOLUTIONS**

[www.htbridge.ch](http://www.htbridge.ch)

**ORIGINAL SWISS ETHICAL HACKING**

Digital Forensics  
Malware Analysis  
Penetration Testing  
Source Code Review  
Security Audit & Consulting

